REQUEST FOR PROPOSAL (RFP)

RFP # 24-021

NEW YORK STATE EDUCATION DEPARTMENT

Title: State Aid Management System Modernization

The New York State Education Department (NYSED) **Office of Management Services (OMS)** is undertaking a significant technology modernization effort by migrating the State Aid Management System (SAMS) from its current legacy platform to a cloud-based low code development platform (LCDP) and a cloud-based Decision Management System (DMS). The SAMS application is critical for identifying and disbursing $30 billion in aid annually to approximately 700 Districts and BOCES in New York State.

SAMS will be the priority of this modernization effort and platform contract. The platforms procured through this contract will initially support SAMS. Subsequent modernization programs may leverage this contract to utilize the LCDP and DMS as shared platforms. The services requested through this RFP will enable NYSED to:

- Become more agile by procuring the platforms and technologies necessary to develop critical solutions.
- Obtain the expertise to build and operationalize these new solutions.
- Improve business processes by utilizing strategic technology enablers.
- Sunset expensive, insecure legacy platforms and technologies.

Two awards are anticipated to result from this RFP. One award will be made to a DMS vendor, and another will be made to a LCDP vendor.

This proposal includes the following deliverables:

- Low Code Development Platform (LCDP)
- Decision Management System (DMS)
- Cloud Infrastructure Services
- Platform Configuration Deliverables
- Staff augmentation

The DMS will provide NYSED the ability to convert critical business rules from legacy code, such as COBOL, to straightforward business-centric executable rulesets. The LCDP will provide NYSED the ability to develop business applications using a turnkey vendor-maintained platform. Using a low-code approach, as opposed to a complex pro-code development platform such as Java, will significantly accelerate business solutioning and drive down application total cost of ownership (TCO).

This proposal is open to vendors who can deliver either the LCDP deliverables or the DMS deliverables, or both:

- If a vendor proposes the LCDP, they must also include proposals for *Cloud Infrastructure Services* and all *Platform Configuration Deliverables*.
- If a vendor proposes the DMS, only requirement #3 of the *Platform Configuration Deliverables* must be proposed.

Additional context regarding the origins of this initiative can be found in the Background portion of Section 1.

NYSED will award one (1) or two (2) contracts pursuant to this RFP, depending on whether the same bidder is awarded both components. The contract(s) resulting from this RFP will be for a five-year term anticipated to begin November 1, 2024 and end October 31, 2029.

Bidders are required to comply with NYSED's Minority and Women-Owned Business Enterprises (M/WBE) participation goals for this RFP through one of three methods. Compliance methods are discussed in detail in the Minority/Women-Owned Business Enterprise (M/WBE) Participation Goals section below.

Service Area**: Statewide**

Mandatory Requirements: See Mandatory Requirements section of the RFP.

Components contained in RFP #24-021 are as follows:

1.) Description of Services to Be Performed
2.) Submission
3.) Evaluation Criteria and Method of Award
4.) Assurances
5.) Submission Documents (separate document)

Questions regarding the request must be submitted by email to rfp24-021@nysed.gov no later than the close of business June 20, 2024. Questions regarding this request should be identified as Program, Fiscal or M/WBE. A Questions and Answers Summary will be posted to the NYSED Procurements webpage no later than July 5, 2024. The following are the designated contacts for this procurement:

Program Matters	**Fiscal Matters**	**M/WBE Matters**
Gabrielle Fisher Brian Waage rfp24-021@nysed.gov	Jessica Hartjen rfp24-021@nysed.gov	Brian Hackett rfp24-021@nysed.gov

Bidders are requested to submit their bids electronically. The following documents should be submitted by email as detailed in the Submission section of the RFP, and must be received at NYSED no later than **July 26, 2024 by 3:00 PM Eastern Time**:

1. Submission Documents (DOCX or PDF) labeled **[name of bidder] Submission Documents RFP #24-021 [either LCDP or DMS]**
2. Technical Proposal (DOCX or PDF) labeled **[name of bidder] Technical Proposal RFP #24-021 [either LCDP or DMS]**
3. Cost Proposal (XLSX) labeled **[name of bidder] Cost Proposal RFP #24-021 [either LCDP or DMS]**
4. M/WBE Documents (DOCX or PDF) labeled **[name of bidder] M/WBE Documents RFP #24-021 [either LCDP or DMS]**

Bidders applying for both LCDP and DMS must submit two separate proposals. LCDP and DMS proposals will be considered separately.

The email address for all the documentation is cau@nysed.gov.

Instructions for Submitting an Electronic Bid:

1. The technical and cost proposal documents should be submitted in Microsoft Office. PDF files that are editable and Optical Character Recognition (OCR) searchable are acceptable. Please do not submit the technical or cost proposal as a scanned PDF.
2. Submission documents requiring a signature must be signed using one of the methods listed below and may be submitted as a Microsoft Office, PDF, or JPG document. A scanned PDF is acceptable for these documents.
3. The following forms of e-signatures are acceptable:
    a. handwritten signatures on faxed or scanned documents
    b. e-signatures that have been authenticated by a third-party digital software, such as DocuSign and Adobe Sign
    c. stored copies of the images of signatures that are placed on a document by copying and pasting or otherwise inserting them into the documents.
4. Unacceptable forms of e-signatures include:
    a. a typed name, including a signature created by selecting a script or calligraphy font for the typed name of the person "signing."
5. To identify the signer and indicate that the signer understood and intended to agree to the terms of the signed document, the signer will sign, or provide by email, the following attestation: "I agree, and it is my intent, to sign this document by [describe the signature solution used] and by electronically submitting this document to [name of recipient individual or entity]. I understand that my signing and submitting this document is the legal equivalent of having placed my handwritten signature on the submitted document and this attestation. I understand and agree that by electronically signing and submitting this document I am affirming to the truth of the information contained therein."
6. In order to ensure the timely receipt of your bid, please use the subject line "BID SUBMISSION RFP 24-021" – failure to appropriately label your bid or submitting a bid to any email address other than the one identified above may result in the bid not being received by the deadline or considered for award.
7. **Bids must be received by 3:00 pm Eastern Time on the due date.**

1.) Description of Services to be Performed

Work Statement and Specifications

This section of the bid package details the services and products to be acquired. Please note that the contract process also includes general New York State administrative terms and conditions, as well as terms and conditions required by New York State law. These terms and conditions address issues related to both the submission of bids and any subsequent contract; they are included separately in this bid package for your information. Please review all terms and conditions.

Mandatory Requirements

The eligible bidder must agree to the Mandatory Requirements found below and must submit the Mandatory Requirements Certification Form, located in 5.) Submission Documents. These required forms must be signed by an authorized person. **Bids that do not comply with the Mandatory Requirements will be disqualified.**

1) All staff augmentation work, as defined in the Staff Augmentation section, must be performed within the Continental United States (CONUS). System and platform support services are exempt from this requirement.
2) The proposed LCDP and DMS platforms must have existed for at least three (3) calendar years.
3) NYSED will own all right, title and interest in all data hosted on the procured platforms.
4) NYSED will own all intellectual property rights of all source code or rulesets produced on behalf of NYSED that was developed through the staff augmentation resources provided through this contract.

Minority and Women-Owned Business Enterprise (M/WBE) Participation Goals Pursuant to Article 15-A of the New York State Executive Law

For purposes of this procurement, NYS Education Department hereby establishes an overall goal of 30% of the total contract amount for M/WBE participation, 17% for Minority-Owned Business Enterprises (“MBE”) participation and 13% for Women-Owned Business Enterprises (“WBE”) participation based on the current availability of qualified MBEs and WBEs. All bidders must document good faith efforts to provide meaningful participation by MWBEs as subcontractors or suppliers in the performance of this Contract. Minority and Women-Owned Business Enterprise (M/WBE) participation includes any and all services, materials or supplies purchased from New York State certified minority and women-owned firms. Utilization of certified Minority and Women-Owned firms will be applied toward the goals. Bidders can achieve compliance with NYSED’s Minority and Women-Owned Business Enterprise goals as described below.

ACHIEVE FULL COMPLIANCE WITH PARTICIPATION GOALS (PREFERRED)
Bidders should submit subcontracting/supplier forms that meet or exceed NYSED’s participation goals for this procurement. All subcontracting/supplier forms must be submitted with the bid proposal. In addition, bidders must complete and submit M/WBE 100: Utilization Plan, M/WBE 102: Notice of Intent to Participate and EEO 100: Staffing Plan. Instructions and copies of these forms are located in the Submission Documents. All firms utilized must be certified with the NYS Division of Minority and Women Business Development before beginning any work on this contract. For

additional information and a listing of currently certified M/WBEs, see the NYS Directory of Certified Minority and Women-Owned Business Enterprises.

The contact person on M/WBE matters is available throughout the application and procurement process to assist bidders in meeting the M/WBE goals. NYSED reserves the right to approve the addition or deletion of subcontractors or suppliers to enable bidders to comply with the M/WBE goals, provided such addition or deletion does not impact the technical proposal and/or increase the total cost of the bid proposal.

DOCUMENTATION OF GOOD FAITH EFFORTS

Bidders must undertake a good faith effort to solicit NYS Certified M/WBE firms as subcontractors and/or suppliers in fulfillment of this procurement. Means of solicitation may include but are not limited to: advertisements in minority centered publications; solicitation of vendors found in the NYS Directory of Certified Minority and Women-Owned Business Enterprises; and the solicitation of minority and women-oriented trade and labor organizations. Bidders will be required to certify and attest to their good faith efforts by completing NYSED's Certification of Good Faith Efforts (Form M/WBE 105). See the M/WBE Submission Documents for detailed examples of and required forms to document good faith efforts.

NYSED reserves the right to reject any bid for failure to document "good faith efforts" to comply with the stated M/WBE goals.

IN THE EVENT BIDDERS CANNOT COMPLY WITH NYSED DESIGNATED PARTICIPATION GOALS, SAID BIDDERS MUST DOCUMENT THEIR "GOOD FAITH EFFORTS" TO COMPLY AND SUBMIT ONE OF THE FOLLOWING REQUESTS:

REQUEST A PARTIAL WAIVER OF PARTICIPATION GOALS

In order to request a partial waiver of the participation goals for this procurement, Bidders must provide documentation of their good faith efforts to obtain the use of certified M/WBE enterprises along with their bid proposal forms. The subcontracting forms must include the participation percentage(s) for which they seek approval. Bidders will be required to certify and attest to their good faith efforts. Bidders should submit a request for a partial waiver (Form M/WBE 101) and document their Good Faith Efforts (Form M/WBE 105) at the same time as the bid is submitted. Bidders must also complete and submit M/WBE 100: Utilization Plan, M/WBE 102: Notice of Intent to Participate and EEO 100: Staffing Plan. The M/WBE Coordinator is available throughout the procurement process to assist in all areas of M/WBE compliance.

REQUEST A COMPLETE WAIVER OF PARTICIPATION GOALS

In order to request a complete waiver of the participation goals for this procurement, Bidders must provide documentation of their Good Faith Efforts to obtain the use of certified M/WBE enterprises along with their bid proposal forms. Bidders will be required to certify and attest to their good faith efforts. Bidders should submit a request for a complete waiver on Form M/WBE 101 and document their Good Faith Efforts (Form M/WBE 105) at the same time as they submit their bid. The M/WBE Coordinator is available throughout the procurement process to assist in all areas of M/WBE compliance.

All payments to Minority and Women-Owned Business Enterprise subcontractor(s) must be reported to NYSED M/WBE Program Unit using M/WBE 103 Quarterly M/WBE Compliance Report. This report must be submitted on a quarterly basis and can be found at NYSED's M/WBE Forms and Compliance Forms webpage.

Service-Disabled Veteran-Owned Business (SDVOB) Participation Goals Pursuant to Article 3 of the Veterans' Services Law

Article 3 of the Veterans' Services Law allows eligible Veteran business owners to get certified as a New York State Service-Disabled Veteran-Owned Business (SDVOB). The goal of Article 3 is to encourage and support eligible SDVOBs to play a greater role in the state's economy by increasing their participation in New York State's contracting opportunities. To this end, NYSED strongly encourages bidders to make maximum possible use of SDVOBs as subcontractors and/or suppliers under this contract, consistent with the requirements of State Finance Law and State procurement guidelines, as well as NYSED policies and procedures. Bidders should consider fulfilling the requirements of this contract through the participation of SDVOBs at a rate of 6%. For additional information about this program, including a list of SDVOBs, please visit the Office of General Services, Division of Service-Disabled Veterans' Business Development website.

Background

The New York State Education Department (NYSED) State Aid Management System (SAMS) is the main application used by NYSED to determine and distribute the correct amount of state aid to public school districts and BOCES throughout the year, as well as to provide accurate and timely data for use in State Aid projections. Today SAMS disburses $30 billion in aid annually to approximately 700 districts and BOCES in NYS. This application is one of several critical technology efforts included in the NYSED IT modernization roadmap.

Beginning in 2003, SAMS was designed and developed to replace a decades-old mainframe system and a temporary data entry assistant system. Large scale SAMS development ceased in 2009 leaving the application straddled between the legacy mainframe, the SAMS Java application writing to a completely different database, and a variety of separate files that had been intended to be temporary. Pain points include requiring maintenance for two disparate applications (including many integrations and data hand-offs needed to support full functionality between two systems and many ancillary processes), ongoing manual data entry by the State Aid team for all paper forms not transitioned to online submission, and increased risk of defects/failure due to 100% custom development required across both applications. In addition, NYSED ITS is at risk of losing key SAMS resources and expertise due to general attrition and retirement which will impact managing the legacy application.

SAMS is comprised of eight modules which sit across the mainframe (MF) and Java application, all of which are in scope for the SAMS Modernization effort and this RFP. The most critical success factor, in addition to addressing pain points addressed above and modernizing the entire application, is continued disbursement of $30B in aid without interruption or issues.

Low Code Development Platform Requirements

The proposed LCDP must be a turnkey Platform as a Service (PaaS) offering that fully enables developer self-service. The subscription costs of the platform and platform components will be invoiced on an annual basis. NYSED may request the addition of ancillary LCDP services, which are listed below, that are not included in the core platform be enabled on the platform. Itemized LCDP ancillary services may be discontinued by NYSED at any time. The subscription cost of the discontinued subcomponents will be prorated from the following year's invoice. The detailed technical requirements are:

- General Requirements:
  - NYSED will have complete operational control over the software development lifecycle (SDLC) of the LCDP service. Further references to a “developer” refer to a NYSED employee or third-party contractor that uses the platform to develop business applications.
- Licensing Requirements:
  - The platform licensing must be based on application complexity. Application complexity is defined by the number of developed user screens, database tables and exposed Application Programming Interface (API) integrations. Licensing must not be based on any per-user basis or metered usage.
  - Support must be included in the base licensing. Please see below for more support requirements.
  - All core functions of the platform must be included in the core subscription. Consuming and providing Representational State Transfer (REST) and Secure File Transfer Protocol (SFTP) services must be included in the core subscription.
  - LCDP Ancillary Services, which are listed below, may be licensed separately from the core subscription. Ancillary features may only provide integration features not included in the core platform. NYSED reserves the right to procure ancillary features on an ad-hoc basis based on our business needs.
  - All individual components of the core LCDP and ancillary LCDP services must be itemized on the provided rate card (see Proposal Documents and Format).
  - NYSED may not be charged for additional infrastructure to support increased platform loads.
- Functional Platform Requirements
  - The platform must provide developers with a Windows desktop client based Integrated Development Environment (IDE).
  - The compilation and deployment of the applications developed on the platform must occur completely on the managed cloud environment. No compilation or deployment should occur on a developer’s workstation.
  - Versioning of applications and components must be completely managed by the core LCDP. Use of external source control systems such as git or Azure DevOps must not be required for the operation of the system. A workflow must be configurable so that a release manager may tag and promote an application to a higher environment.
  - The platform must support five (5) environments: development (DEV), quality assurance (QA), staging (STAGE), production (PROD) and disaster recovery (DR).
  - The LCDP must provide developers the ability to create bespoke relational data models. Data modelling must be implemented using a graphical user interface (GUI) provided within the IDE. No textual Structured Query Language (SQL) or Data Definition Language (DDL) should be required to develop data models for applications.
  - The LCDP must support the development of reactive web applications and native mobile applications.
  - Business logic must not require textual code besides declaring values to objects or variables. All business logic must be developed using a GUI within the IDE. Custom business logic may be required to be developed to ensure data integrity.
  - Development of an application user interface (UI) must be developed using a what-you-see-is-what-you-get (WYSIWYG) GUI provided by the IDE. Create, read, update and delete (CRUD) operations must be implemented using turnkey “drag and drop” operations.
  - Developing UIs must not require knowledge or expertise in Hypertext Markup Language (HTML), JavaScript or Cascading Stylesheets (CSS). However, UI templates must be

customizable and reusable. HTML, JavaScript and CSS may be required to customize UI templates.
    - Deployments between environments, such as DEV to QA, QA to STAGE, and STAGE to PROD, must be completely managed within the platform. External tools, such as Jenkins must not be required to implement continuous deployment processes.
    - Integrations with external Representational State Transfer (REST) services must not require development of textual programming code. Integrations with external REST services must be natively supported by the platform.
    - All core functions of the core platform must be invokable through a REST service and a self-service web portal.
- Infrastructure Requirements
    - NYSED will be utilizing the turnkey LCDP directly provided by the vendor. However, the LCDP must fully support a hybrid cloud strategy. The LCDP must be available as a turnkey platform provided by the platform vendor or deployable on infrastructure that is provisioned and managed by NYSED or a third-party provider.
    - The LCDP must allow for continued operation of NYSED developed applications even if the LCDP subscription is terminated or the LCDP provider ceases business operations. NYSED will need to provide its own infrastructure in these circumstances.
    - Virtual private network (VPN) connections must be available to securely connect the LCDP with the NYSED data center or a cloud provider of NYSED's choosing.
- LCDP Ancillary Services:
    - As stated above, each of these features are licensed separately from the core platform. These features will be licensed at the full discretion of NYSED. Each feature will be licensed separately and will be invoiced annually.
    - An option must be available to replicate all transactional business data that persists within the platform in near-real time. The replicated data must be stored in a read-only staging relational database. NYSED must have unfettered access to this staging database to implement a variety of analytical or reporting use cases.
    - An option must be available to stream all log and audit data, in near real time, from the platform to a third-party log management platform[1] of NYSED's choosing.
    - An option must be available to use a turnkey NoSQL, document-based PaaS database, comparable to MongoDB Atlas. The LCDP must support direct integration with this NoSQL service.
    - An option must be available to use cloud object storage, comparable to Amazon Web Services (AWS) S3. The LCDP must support direct integration with object storage service.

Decision Management System Platform Requirements

The proposed DMS must be a turnkey, cloud-based PaaS offering. The DMS must support the development of business rules and financial calculations using an easy to learn development environment. We anticipate that the initial project will require 35,000 production calculations annually. Of the 33,000 calculations, 8,400 are highly complex. These calculations will be executed during the Payment periods, which are specified in the Production Blackout Schedule attached to the RFP. The Proposal should include the subscription model in which the DMS will be licensed. Detailed requirements are as follows:

- General Requirements:
    - Deployment of the DMS and supported rulesets must not require experience or knowledge of any pro-code development frameworks (such as Java, .Net or Python).

[1] Splunk, for example.

Configuration or manual installation of any underlying infrastructure, such as application servers, web servers or databases, must not be required for the operation of the DMS.

- Licensing Requirements:
  - While the DMS may be available within a suite of development products, such as a sub-component of a larger Business Process Management System (BPMS), the procurement and operation of the entire suite must not be a requirement of the Proposal.
  - The DMS subscription may not be based on the number of end users (end users are humans that invoke the execution of rule sets).
- Functional Platform Requirements:
  - Ruleset development must occur on a web-based environment. Microsoft Office applications with a supported rules editing plugin may also be provided as an acceptable rules development environment. An IDE must not be required to develop rulesets.
  - The DMS must produce graphical representations of rulesets. The ability to model and review rulesets using Decision Model and Notation (DMN) is preferred.
  - The DMS must support the following approaches for rules authoring or development:
    - Drag-and-drop logic modelling
    - Truth tables
    - Textual equations

    Natural language rule definitions may be provided in lieu of drag-and-drop modelling and textual equations.
  - The DMS platform must allow for non-persistent, idempotent testing of rulesets. The DMS must support usage audits. However, ruleset tests do not need to be persisted by the DMS platform.
  - The DMS platform must support a simulation feature that allows rules developers to run What-If rules analyses.
  - Versioning of rulesets must be completely managed by the DMS platform. Use of external source control systems, such as git or Azure DevOps, must not be required for the operation of the system. The DMS platform must allow developers to develop, test and execute rulesets while a "production" version of the ruleset is used by the system of record. A workflow must be configurable so that a release manager may tag and promote a ruleset to be used by a system of record. Versioning of rulesets must not require additional environments or infrastructure.
  - The DMS must support temporal rulesets, which means that time must be available as a parameter for rule logic.[2]
  - The DMS must provide multiple ways to test rulesets. While rulesets may be tested programmatically, this must not be a requirement. Required test options include:
    - A web interface where a developer or tester can manually input test values and view test results. This test method must provide a graphical debugger that explains the test results visually. Test inputs should be saved for subsequent test activities.
    - The DMS must support an import tool where Microsoft Excel spreadsheets or Comma-Separated Values (CSV) files with input values may be uploaded. After the file is uploaded, the ruleset results will be appended to the spreadsheet and downloadable by the user.
  - All "production" rulesets must be invokable from a REST API. The REST API must behave consistently between rulesets. The REST API must not require manual provider-side or consumer-side deployment steps after the release of new rulesets.[3] The REST API should be protected using OAuth 2.0 authentication or an API key. If API keys are utilized,

[2] For example: A rule may state that a result will have a value of zero (0) prior to January 1st, 2024, and the same rule will result with a value of a thousand (1000) on and after January 1st, 2024.

[3] The interface that is used to expose the REST API must not change after rulesets are changed.

they must be transferred using POST HTTP headers. API consumer authorization must be managed through the DMS provided configuration portal.
    - All rulesets must be exportable to an open external file format, such as JSON or XML.

Common Platform Requirements

The following are platform requirements that must be met by both the LCDP and the DMS:

- Licensing and Subscription Requirements:
    - The underlying infrastructure of the platform, such as servers, databases, networking (including traffic egress and ingress), and storage, must be included in the core licensing.
    - Support must be included in the base licensing. Please see below for more support requirements.
    - NYSED may not be charged for additional infrastructure to support increased platform loads.
    - Training for the platform must be provided with the core platform subscriptions. This must include self-paced web-based training, reference manuals, knowledge base access and remote instructor-led training. Training must include one-time instructor led training for 20 developers and five (5) platform administrators. Each training attendee must be provided one voucher for in-person[4] platform certification. Training will be provided within the first year of the contract.
- Quality of Service (QoS) Requirements:
    - The vendor must fully operate and manage the underlying infrastructure that supports the provided platform.
    - The platform must maintain a 99.95% uptime.
    - The vendor must maintain all components of the platform and the underlying infrastructure. All maintenance work must occur outside the payment periods that are specified in the Production Blackout Schedule attached to the RFP. The vendor must notify the Authorized User contact list 30 days prior to a scheduled change. For security related patches, the NYSED contact list must be notified as soon as possible to schedule an emergency change.
- Service Level Agreement:
    - In the event of an issue, NYSED requires the following response expectations:

Issue Severity	Maximum Response Time from the Vendor after each Correspondence	Availability
Any Production Issue	1 Hour	24/7/365
Any Issue Blocking Development	24 Hours	Monday through Friday excluding State Holidays
Any Other Issue	2 Business Days	Monday through Friday excluding State Holidays

Table 1: Support Service Level Agreement

- Security and Compliance Requirements:
    - The platform must support integration with any NYSED supported Identity Provider (IDP) using the Security Assertion Markup Language (SAML) version 2 or the Open Identity Connect (OIDC) protocols. All end-user authentication must be implemented through this integration with this IDP.
    - The platform must support NYS Education Law § 2-d compliance. Compliance is only required when the platform persists or transfers Student Data through the system.

[4] NYSED staff has had poor experiences with remote test proctoring services.

- The platform must support Health Insurance Portability and Accountability Act (HIPAA) compliance. HIPAA compliance controls will only be required when the platform persists or transfers Health Information through the system.
- Core business data[5] may not leave the Continental United States (CONUS) without express written authorization from NYSED. Application metadata, source code and logging information may leave CONUS to utilize support services that are provided by the vendor.
- All data in transit and at rest must be encrypted.
- All cryptographic algorithms and technologies must comply with Federal Information Processing Standards (FIPS) 140-2 requirements. Therefore, all cryptographic algorithms and technologies must be upgraded when more secure alternatives are developed.
- All applicable controls listed in the following Information Security policies and standards must be implemented. These documents are attached to this RFP.
  - Acceptable Use Policy
  - Appendix R (Data Security and Privacy Plan Provisions)
  - Cyer Incident Response Standard
  - Cybersecurity Incident Response Policy
  - Data Classification Policy
  - Data Privacy and Security Policy
  - Encryption Standard
  - Firewall Policy
  - Information Security Policy
  - Secure Disposal Standard
  - Secure Remote Access Standard
  - Service Account Password Policy

- Data Ownership and Intellectual Property Requirements:
  - NYSED will own all right, title and interest in all data hosted on the platform.
  - NYSED will own all intellectual property rights of the application code developed on the platform.
  - The terms of this contract supersede any terms and conditions asserted on any plugin or component that is provided by the vendor on any vendor supported plugin marketplace. This requirement does not apply to plugins that are not owned by the vendor.
- Business Continuity and Disaster Recovery Requirements
  - The Recovery Point Objective (RPO) and Recovery Time Objective (RTO) are both 24 hours from the declaration of a disaster. The vendor must provide written Disaster Recovery procedures within the first 30 calendar days of the engagement.
  - The vendor must keep a replicate instance of the production databases and codebases within a separate geographical region as the primary operational database. A separate daily backup of the production database must be stored in an air gapped third party location. This backup location will be provided by NYSED.
  - Disaster Recovery procedures must be tested twice a year. These tests will be mutually scheduled by NYSED and the vendor. A Disaster Recovery test may not be scheduled during a blackout period.

Cloud Infrastructure Services

Applications developed on the LCDP may require supplemental infrastructure technology services to fulfill business requirements. For example, NYSED may need to develop a serverless utility function

[5] Core Business Data is defined as any data that is used by the application to fulfil any end-user business purpose. Core business data generally includes all data except logs, source code and other technical meta-data.

using a PaaS service comparable to AWS Lambda. These services must be available on the same tenant that hosts the LCDP. The services will be configured by NYSED using self-service configuration provided by the underlying cloud provider. The vendor will enforce safeguards that will prevent operational disruptions to the LCDP. The vendor will prepare the environment for NYSED by implementing the following deliverables:

- Provision NYSED administrative accounts and configuring administrative authorization. All administrative access must follow NYSED security policy.
- Provision support accounts with the underlying cloud provider. Support issues may be submitted by NYSED. The vendor may track issues submitted by NYSED for operational awareness.

All applicable controls listed in the following Information Security policies and standards must be implemented. These documents are attached to this RFP.

- Acceptable Use Policy
- Appendix R (Data Security and Privacy Plan Provisions)
- Cyber Incident Response Standard
- Cybersecurity Incident Response Policy
- Data Classification Policy
- Data Privacy and Security Policy
- Encryption Standard
- Firewall Policy
- Information Security Policy
- Secure Disposal Standard
- Secure Remote Access Standard
- Service Account Password Policy

Platform Configuration Deliverables

The following is a list of fixed cost deliverables for the initial configuration and development of the LCDP. Proposals for the DMS platform must also include deliverable #3. NYSED reserves the right to determine if the vendor will be assigned to perform a deliverable. A formal task order will be provided to the vendor prior to the start of any deliverable. The vendor will submit an invoice for each completed deliverable. Completion of a deliverable must be reviewed and approved by the SAMS Project Director prior to an invoice. The vendor will maintain continuity of staff throughout the course of each engagement. All changes in staff will be subject to NYSED approval.

1) Implementation of the NYSED Style Guide. The NYSED style guide is accessible at this URL: https://eservices.nysed.gov/nysed-assets/color_scheme.html. A turnkey reusable component must be available for use by application developers to develop business applications on the LCDP using the reusable Style Guide implementation component. An instruction manual must also be provided by the vendor on how to use the developed components. Ongoing support for the style components must be provided by the Provider throughout the duration of the contract period. This will be a one-time fixed deliverable. This deliverable will be invoiced once the deliverable requirements are implemented and deployed to the production environments.
2) Production replication to Staging. All data for a given application developed on the LCDP must be synchronized between the production environment and the staging environment. A framework must be developed that will allow NYSED to enable this synchronization for a set of applications that require this feature. Enablement and disablement of the synchronization must be configurable by NYSED technical staff. The synchronization must be executed nightly at a time determined by NYSED. Data from the production version of the application will be directly replicated into the staging instance of the application. Deployment constraints may be

configured to ensure that the application versions of production and staging are identical. An instruction manual of the replication component must also be provided by the vendor. Ongoing support for the replication component must be provided by the vendor throughout the duration of the contract period. This feature must support the deployment of emergency production deployments during business hours. This will be a one-time fixed deliverable. This deliverable will be invoiced once the deliverable requirements are implemented and deployed.

3) Inclusion of additional services or a customer success program for the initial implementation of the LCDP or DMS (whichever is applicable for the proposal). These services will include solution architecture review, additional development support by platform experts, code reviews and code support. Support for components that are provided by the LCDP and DMS vendors must also be included where applicable. This service should include a dedicated customer success manager for each platform. This service must be provided through a standard annual rate and should include a set of hours for support, with a minimum of 2,000 hours. The vendors must have the ability assign subject matter experts (SME) to address individual issues. These deliverables are fixed-price deliverables. They will be invoiced annually at the start of the engagement. NYSED has full discretion to renew this service on an annual basis.

Staff Augmentation

In addition to the technology components required for the Proposal, we will need staff augmentation services to develop and support the business applications that are developed on the platforms. Staff Augmentation Requirements:

1) Vendor supplied staff will be charged on an hourly basis and will be invoiced monthly. NYSED will provide a task order for each role that needs to be fulfilled. Within five (5) business days, the assignee will provide three (3) to five (5) resumes of available candidates. The NYSED staff will interview one or more candidates. The interviews will occur remotely over video conference. After the interviews are concluded, NYSED will either select a candidate or request more candidates. The NYSED Project Director will appoint an interview panel comprised of NYSED staff to conduct the interviews or will assign an individual to conduct the interviews. Interview questions and scoring metrics will be at the full discretion of the NYSED.
2) Once a candidate is selected, NYSED will issue a task order to the vendor. The candidate is expected to begin work within five (5) business days after a task order is issued.
3) Staff hours may be invoiced on a monthly basis. Roles are defined in the Staff Roles section below. Rates must match the rates included in the cost proposal for the specified role.
4) Staff selected through this process may be released at-will, without notice, for any reason determined by NYSED. Terminated staff are expected to return NYSED equipment through a major shipping carrier within 24 hours (regardless of the day or time).
5) NYSED projects that the number of annual staff hours that will be utilized annually will be 15,000 hours for the LCDP vendor and 10,000 hours for the DMS vendor.
6) NYSED will retain the sole discretion of the appropriate staffing levels for its ongoing projects.

Staffing Roles

The following is the list of staffing roles that must be provided by the vendor. These roles will be used for Staff Augmentation.

Role	Applicable Contract	General Description of Activities[6]	Required Qualifications
Project Manager	Both	• Establish and manage the overall vendor project plan and schedule. • Act as SAMS Modernization implementation team daily counterpart by responding to emails, joining daily standups and weekly statuses as needed. • Answer all project related questions on behalf of the vendor. • Define sprints based upon team capacity and velocity, track burndown, conduct sprint ceremonies. • Lead weekly status with SAMS implementation team and business stakeholders. • Ensure requirements, user stories, and acceptance criteria are understood by vendor. • Manage schedule, cost, efforts, quality of deliverables and risks/contingency planning. • Provide weekly burn reports of actual vs forecast hours, and compare to project percent complete, and provide mitigation plan if + or – 10% variance. • Facilitate management and technical meetings, sending meeting notes and tracking action items. • Develop and implement project management processes, tools and	• Experience leading complex modernization initiatives spanning across multiple teams and vendors. • Demonstrate successful experience leading large scale platform migrations and implementations. • Extensive experience managing large budgets and tracking both spend and project burn. • Excellent verbal and written communication. • Demonstrate ability to manage multiple priorities across multiple teams. • Experience using Jira, Confluence, Smartsheet and SharePoint. • Excellent stakeholder management capabilities and experience working in a “no surprises” environment. • Ability to create and manage large Gantt timelines with many moving parts and dependencies.

[6] These activities are described for illustrative purposes. Absence of an activity in this section does not justify a change order or change in hourly rate.

		artifacts using Jira/Confluence, MPP, SharePoint, Visio, and LucidChart.	
Development Lead	Both	• Supervise vendor development staff. • Monitors issues, tasks, other activities in JIRA. • Mentor NYSED development staff. • Provide technical specifications to development staff. • Enforce coding, security, and other technical standards. • Advise NYSED technical staff to collaboratively design technical solutions. • Reviews and deploys applications to the QA environment.	• Extensive expertise and knowledge in the provided LCDP or DMS. • Previous experience in Java (preferred), C#, Python, or another pro-code development platform. • Previous experience with REST API, relational databases, data migrations from legacy systems, log management, NoSQL database technologies and web design. • Supervisory experience of development staff. • Must have experience using JIRA and Confluence.
Low-Code Developer	LCDP	• Develops business applications, unit tests and shared components on the provided LCDP.	• Development experience on the provided LCDP. Developers with applicable LCDP certifications are preferred. • Must have experience using JIRA and Confluence.
Rules Modeler/Developer	DMS	• Develops business rules and test suites on the provided DMS. • Collaborates directly with SAMS program staff to develop and test business rules.	• Development or modelling experience on the provided DMS. Developers with applicable DMS certifications are preferred. • Must have a strong business analysis acumen. Previous experience in the accounting or finance related field is preferred. • Experience with COBOL is preferred. • Must have experience using JIRA and Confluence.
UX/Web Specialist	LCDP	• Develops or refines web components using the LCDP and based on provided wireframes and site map. • Tests and fixes issues relating to 508 Accessibility compliance.	• Experience with the provided LCDP. • Extensive experience with CSS, HTML5 and JavaScript. • Experience testing and fixing 508 accessibility compliance issues. • Must have experience using JIRA and Confluence.
Pro-Code Developer	LCDP	• Develops required applications or components in Java.	• Experience with Spring Boot, IntelliJ, Jenkins, git, Gradle and Maven.

			• Experience with Vue.js. • Experience developing REST API. • Experience developing PL/SQL.
Training Specialist	Both	• Develops detailed end-user manuals and other training materials for newly released business applications. • Delivers end user training to various groups, either directly or through a Train the Trainer approach.	• Experience authoring and editing training documents, knowledge articles and other technical documentation needed for training purposes. • Experience delivering training to various audiences.
Platform Specialist	Both	• Configures the LCDP or DMS according to specification. • Creates and configures system health monitoring for the LCDP, DMS or other cloud-based infrastructure. • Troubleshoots and resolves issues with the LCDP and DMS platforms.	• Experience with the provided LCDP or DMS. • Administrative experience with the IaaS platform that supports the LCDP.
Cloud Specialist	LCDP	• Develop infrastructure provisioning and other administrative capabilities using Terraform. • Creates and configures system health monitoring for cloud PaaS or IaaS services. • Troubleshoot and resolve issues with the PaaS or IaaS services.	• Administrative experience with the IaaS platform that supports the LCDP. • Experience with Terraform. • Experience with shell scripting, PowerShell or similar scripting coding languages. • Experience configuring a wide range of web infrastructure components such as web servers, application servers, and load balancers.
Quality Control Specialist	Both	• Develop test plans based on documented business requirements and acceptance criteria. • Develop automated functional test scripts using Katalon, Selenium or similar. • Develop integration tests using Hoppscotch or Postman.	• Experience developing test plans and analyzing business requirements. • Experience with Katalon, Selenium or similar. • Experience with Hoppscotch or Postman. • Experience with JMeter or creating load-test scripts.

	• Develop load tests using JMeter. • Review unit tests create by development staff.

Table 2: Staff Augmentation Roles

All staff augmentation work described in this section will occur remotely within CONUS. The vendor must be available during NYSED business hours which are 8:00 AM to 5:00 PM Monday through Friday, excluding State holidays. All staff must be available 24/7/365 to address production issues if they arise.

All vendor staff must perform all work on NYSED issued laptops, which will be shipped to the vendor staff. All equipment must be returned to NYSED within 24 hours after an engagement has been completed, regardless of the date or time. All equipment must be shipped through a major shipping carrier.

All vendor staff must use NYSED provided accounts to perform all in-scope work relating to this RFP. Vendor staff must use the following software that is provided by NYSED when applicable:

- Microsoft Outlook, including using a NYSED provided email account for all email correspondence
- Microsoft Teams, including using a NYSED provided Teams account for all Instant Message (IM) correspondence
- Confluence for documentation
- JIRA for task and issue tracking
- SharePoint for document collaboration
- IntelliJ IDEA for Pro-code development
- Git and Bitbucket for source control, where applicable

Where applicable, all vendor staff is expected to perform the core functionalities of these listed tools. All vendor staff is expected to perform basic operations of the Windows 10 operating system. No technology training will be provided to vendor staff. The vendor may not charge NYSED for any staff training activities.

In the event where NYSED must change one of these listed platforms, the vendor will be given three (3) months' notice prior to the migration. A migration strategy will be developed between the vendor and NYSED.

NYSED reserves the right hire any vendor provided staff member as a full-time employee. Candidates may only be hired through standard Civil Service procedures.

All work and deliverables must be performed according to development and project management standards provided by NYSED. These standards will be provided to the vendor within 30 days of the issuance of the contract. We cannot provide development or project management standards with this RFP because NYSED does not know what the provided platforms are yet. Requirements are also in progress and will be provided to the contractor at the start of implementation.

All project documentation, including requirements, will be managed on a NYSED provided Confluence instance. All task tracking will be managed on a NYSED provided JIRA instance. When applicable, source code will be managed on a NYSED managed git or BitBucket instance.

NYSED will never be charged for travel expenses without explicit authorization, which will be evaluated on a case-by-case basis. When travel is required by NYSED, expenses for travel, lodging, and subsistence shall be reimbursed at the per diem rate in effect at the time for New York State Management/Confidential employees.

When applicable, NYSED prefers that all Gantt charts be provided in Smartsheet.

Data Privacy Appendix

The New York State Education Department's Data Privacy Appendix (Appendix R) is annexed to this RFP, the terms of which are incorporated herein by reference, and shall also be part of the Contract.

Bidders should use the templates and instructions in Appendix R to submit the required DPA EXHIBIT 1 - Contractor's Data Privacy and Security Plan and return it with their proposal for review.

Accessibility of Web-Based Information and Applications

Any documents, web-based information and applications development, or programming delivered pursuant to the contract or procurement, will comply with New York State Education Department IT Policy NYSED-WEBACC-001, Web Accessibility Policy as such policy may be amended, modified or superseded, which requires that state agency web-based information, including documents, and applications are accessible to persons with disabilities. Documents, web-based information and applications must conform to NYSED-WEBACC-001 as determined by quality assurance testing. Such quality assurance testing will be conducted by NYSED employee or contractor, and the results of such testing must be satisfactory to NYSED before web-based information and applications will be considered a qualified deliverable under the contract or procurement.

Subcontracting

For vendors using subcontractors, a Vendor Responsibility Questionnaire and a NYSED vendor responsibility review are required for a subcontractor when:

- The subcontractor is known at the time of the contract award.
- The subcontractor is not an entity that is exempt from reporting by OSC.
- The subcontract will equal or exceed $100,000 over the life of the contract.

For additional information about Vendor Responsibility, see the **Vendor Responsibility** section contained in **3.) Evaluation Criteria and Method of Award** of this RFP.

If the vendor proposes to change subcontractors during the contract period, NYSED must be notified prior to the change. NYSED reserves the right to reject any replacement subcontractors proposed by the vendor and reserves the right to approve all changes in subcontractors. The Subcontracting Form located in the Submission Documents must be updated annually and submitted to NYSED. Using this form, the vendor must also report to NYSED, on an annual basis, actual expenditures incurred for all subcontractors and indicate which subcontracting costs are associated with M/WBE.

Contract Period

NYSED will award one (1) or two (2) contract(s) pursuant to this RFP, depending on whether the same bidder is awarded both components. The contract(s) resulting from this RFP will be for a five-year term anticipated to begin November 1, 2024 and to end October 31, 2029

Electronic Processing of Payments

In accordance with a directive dated January 22, 2010, by the Director of State Operations – Office of Taxpayer Accountability, all state agency contracts, grants, and purchase orders executed after February 28, 2010, shall contain a provision requiring that contractors and grantees accept electronic payments.

M/WBE and Equal Employment Opportunities Requirements:
Contractor Requirements and Obligations under New York State Executive Law, Article 15-A (Participation by Minority Group Members and Women with Respect to State Contracts)

In an effort to eradicate barriers that have historically impeded access by minority group members and women in State contracting activities, Article 15-A, of the New York State Executive Law §310-318, (Participation By Minority Group Members and Women With Respect To State Contracts) was enacted to promote equality of economic opportunities for minority group members and women.

The New York State Education Department ("NYSED") has enacted its policies Equal Opportunity, Non-Discrimination and Affirmative Action and on Minority and Women-Owned Business Enterprise Procurements consistent with the requirements as set forth under the provisions of Article 15-A (the "Article") incorporated by reference, requiring Contracting Agencies to implement procedures to ensure that the "Contractor" (as defined under Article 15-A, §310.3 shall mean an individual, a business enterprise, including a sole proprietorship, a partnership, a corporation, a not-for-profit corporation, or any other party to a state contract, or a bidder in conjunction with the award of a state contract or a proposed party to a state contract, complies with requirements to ensure Equal Employment Opportunities for Minority Group Members and Women, in addition to providing Opportunities for Minority and Women-Owned Business Enterprises on all covered state contracts.

In keeping with the intent of the Law, it is the expectation of the Commissioner and the responsibility of all contractors participating in and/or selected for procurement opportunities with NYSED, to fulfill their obligations to comply with the requirements of the Article and its implementing regulations.

In accordance with these requirements, the contractor hereby agrees to make every good faith effort to promote and assist the participation of certified Minority and Women-Owned Business Enterprises ("M/WBE") as subcontractors and suppliers on this project for the provision of services and materials in an amount at least equal to the M/WBE goal (Included in the procurement document) as a percentage of the total dollar value of this project. In addition, the contractor shall ensure the following:

1. All state contracts and all documents soliciting bids or proposals for state contracts contain or make reference to the following provisions:

    a. The contractor will not discriminate against employees or applicants for employment because of race, creed, color, national origin, sex, age, disability, marital status, gender, religion, veteran status, sexual orientation, genetic disposition or carrier status and will undertake or continue existing programs of affirmative action to ensure that minority group members and women are afforded equal employment opportunities without discrimination.

        For purposes of the Article, affirmative action shall mean recruitment, employment, job assignment, promotion, upgrading, demotion, transfer, layoff or termination and rate of pay or other forms of compensation.

b. The contractor shall request each employment agency, labor union, or authorized representative of workers with which it has a collective bargaining or other agreement or understanding, to furnish a written statement that such employment agency, labor union or representative will not discriminate on the basis of race, creed, color, national origin, sex, age, disability, marital status, gender, religion, veteran status, sexual orientation, genetic disposition or carrier status and that such union or representative will affirmatively cooperate in the implementation of the contractor's obligation herein.

c. The contractor shall state in all solicitations or advertisements for employees, that, in the performance of the State contract, all qualified applicants will be afforded equal employment opportunities without discrimination because of race, creed, color, national origin, sex, age, disability, marital status, gender, religion, veteran status, sexual orientation, genetic disposition or carrier status.

2. The contractor will include the provisions of subdivision one of this section in every subcontract as defined under §310.14, except as provided under §312.6 of the Article, in such a manner that the provisions will be binding upon each subcontractor as to work in connection with the State contract.

3. Contractors or subcontractors shall comply with the requirements of any federal law concerning equal employment opportunity, which effectuates the purpose of this section.

4. Contractors and subcontractors shall undertake programs of affirmative action and equal employment opportunity as required by this section[7]. In accordance with the provision of the Article, the bidder will submit, with their proposal, Staffing Plan (EEO 100).

5. Certified businesses (as defined under Article 15-A, §310.1 means a business verified as a minority or women-owned business enterprise pursuant to §314 of the Article) shall be given the opportunity for meaningful participation in the performance of this contract, to actively and affirmatively promote and assist their participation in the performance of this contract, so as to facilitate the award of a fair share of this contract to such businesses.

6. Contractor shall make a good faith effort to solicit active participation by enterprises identified in the Empire State Development ("ESD") directory of certified businesses. The contractor must document its good faith efforts as set forth in 5 NYCRR 142.8. This document, Contractors Good Faith Efforts, can be found in the M/WBE Submission Documents.

7. Contractor shall agree, as a condition of entering into said contract, to be bound by the provisions of Article 15-A, §316.

8. Contractor shall include the provisions set forth in paragraphs (6) and (7) above in every subcontract in a manner that the provisions will be binding upon each subcontractor as to work in connection with this contract.

9. Contractor shall comply with the requirements of any federal law concerning opportunities for M/WBEs that effectuates the purpose of this section.

10. Contractor shall submit all necessary M/WBE documents and/or forms as described above as part of their proposal in response to NYSED procurement.

[7] Notice – Contractors are provided with notice herein, NYSED may require a contractor to submit proof of an equal opportunity program after the proposal opening and prior to the award of any contract. In accordance with regulations set forth under Article 15-A §312.5, contractors and/or subcontractors will be required to submit compliance reports relating to the contractor's and/or subcontractor's program in effect as of the date the contract is executed.

11. The percentage goals established for this RFP are based on the overall availability of M/WBEs certified in the particular areas of expertise identified under this RFP. These goals should not be construed as rigid and inflexible quotas that must be met, but as targets reasonably attainable by means of applying every good faith effort to make all aspects of the entire Minority and Women-Owned Business Program work.

12. Contractor shall ensure that enterprises have been identified (M/WBE 102) within the Utilization Plan, and the contractor shall attempt, in good faith, to utilize such enterprise(s) at least to the extent indicated in the plan, as to what measures and procedures contractor intends to take to comply with the provisions of the Article.

13. Upon written notification from NYSED M/WBE Program Unit as to any deficiencies and required remedies thereof, the contractor shall, within the period of time specified, submit compliance reports documenting remedial actions taken and other information relating to the operation and implementation of the Utilization Plan.

14. Where it appears that a contractor cannot, after a good faith effort, comply with the M/WBE participation requirements, contractor may file a written application with NYSED M/WBE Program Unit requesting a partial or total waiver (M/WBE 101) of such requirements setting forth the reasons for such contractor's inability to meet any or all of the participation requirements, together with an explanation of the efforts undertaken by the contractor to obtain the required M/WBE participation.

For purposes of determining a contractor's good faith efforts to comply with the requirements of this section or be entitled to a waiver, NYSED shall consider at the least the following:

1. Whether the contractor has advertised in general circulation media, trade association publications and minority-focused and women-focused media and, in such event:

    a. Whether or not the certified M/WBEs which have been solicited by the contractor exhibited interest in submitting proposals for a particular project by attending a pre-bid conference; and

    b. Whether certified businesses solicited by the contractor responded in a timely fashion to the contractor's solicitations for timely competitive bid quotations prior to the contracting agency's deadline for submission of proposals.

2. Whether there has been written notification to appropriate certified M/WBEs that appear in the Empire State Development website.

All required Affirmative Action, EEO, and M/WBE forms to be submitted along with bids and/or proposals for NYSED procurements are attached hereto. Bidders must submit subcontracting forms that:

1. fully comply with the participation goals specified in the RFP *OR*

2. partially comply with the participation goals specified in the RFP, and include a request for partial waiver, and document their good faith efforts to fully comply with the percentage goals specified in the RFP *OR*

3. do not include certified M/WBE subcontractors or suppliers, and include a request for a complete waiver, and document their good faith efforts to fully comply with the participation goals specified in the RFP.

All M/WBE firms are required to be certified by Empire State Development (ESD). Online Certification can be found at the New York State Contract System website.

Failure to comply with the requirements of Article 15-A as set forth under this procurement and in conjunction with the corresponding contract, will result in the withholding of associated funds and other enforcement proceedings set forth under Article 15-A.

2.) Submission

Documents to be submitted with this proposal

This section details the submission document or documents that are expected to be transmitted by the respondent to the State Education Department in response to this RFP. New York State Education Department shall own all materials, processes, and products (software, code, documentation and other written materials) developed under this contract. Materials prepared under this contract shall be in a form that will be ready for copyright in the name of the New York State Education Department. Any subcontractor is also bound by these terms. The submission will become the basis on which NYSED will judge the respondent's ability to perform the required services as laid out in the RFP.

Proposal Submission

Proposals submitted in response to this RFP must include the following documents submitted by email to cau@nysed.gov per the electronic proposal submission procedures outlined above, preferably with each of the following sets of documents attached as a single file (i.e. one email with four attachments):

1) Submission Documents bearing signature
2) Technical Proposal (DOCX or PDF)
3) Cost Proposal (Filled out Excel File)
4) M/WBE Documents bearing signature

Bidders applying for both LCDP and DMS must submit two separate proposals. LCDP and DMS proposals will be considered separately.

Proposals must be received by **July 26, 2024 by 3:00 PM** by email to cau@nysed.gov.

Proposals should be prepared simply and economically, avoiding the use of elaborate promotional materials beyond those sufficient to provide complete presentation. If supplemental materials are a necessary part of the proposal, the bidder should reference these materials in the technical proposal, identifying the document(s) and citing the appropriate section and page(s) to be reviewed.

The proposal must communicate an understanding of the deliverables of the RFP, describe how the tasks are to be performed, identify potential problems in the conduct of the deliverables and methods to identify and solve such problems.

Bidders should specify all details and dates required to evaluate the technical proposal and should limit aspects of the project plan that are to be determined only after the award of a contract.

Any proprietary material considered confidential by the bidder will specifically be so identified, and the basis for such confidentiality will be specifically set forth in the proposal by submitting the form "Request for Exemption from Disclosure Pursuant to the Freedom of Information Law," located in 5) Submission Documents.

Proposal Documents and Format

The proposal should be provided in the format described in this section. Proposals should be written in a document format. Use of slide decks are discouraged. Unnecessary attachments that do not directly fulfill the required format will not be evaluated and are discouraged. Each page of the proposal should state the name of the proposer, the RFP number, LCDP or DMS, and the page number.

The completed Technical Proposal should be labeled **[Name of Bidder] – Technical Proposal – RFP #23-021 – [either LCDP or DMS]** and include the following:

1) Executive Summary: This section should not exceed one page. This section is required for all proposals.
2) Proposers General Qualifications: This section must include the following:
    a. Highlight the Proposer's experience fulfilling similar engagements. This must include previous a list of government and private sector clients, along with a case study describing each engagement.
    b. A list of potential sub-contractors and their role in the proposal.
    c. A list of five (5) or more client references, including email and telephone number. At least one reference must be a State, Local or Education (SLED) organization.

    This section is required for all proposals.
3) LCDP Proposal: This section must state the name of the LCDP and describe the proposed LCDP. Every requirement in the Low Code Development Platform Requirements and Common Platform Requirements sections must be addressed. If any of these stated requirements cannot be met by the proposed LCDP, the Proposer must disclose and explain the shortcoming and provide a proposed solution for mitigating the lack of capability. The Proposer may not charge NYSED for mitigating solutions. This section is required for all LCDP proposals.
4) DMS Proposal: This section must state the name of the DMS and describe the proposed DMS. Each requirement in the Decision Management System Requirements and Common Platform Requirements sections must be addressed. If any of the stated requirements cannot be met by the proposed DMS, the Proposer must disclose and explain the shortcoming and provide a proposed solution for mitigating the lack of capability. The Proposer may not charge NYSED for mitigating solutions. This section is required for all DMS proposals.
5) Cloud Infrastructure Services Proposal: This section will identify the proposed cloud platform described in the Cloud Infrastructure Services section. The core provider must be identified in this section. This section should include a detailed technical description on how this deliverable will be met by the Proposer. If provided services are available through the General Services Administration (GSA) or New York State (NYS) Umbrella contract, the proposed costs may not exceed established GSA or NYS Umbrella contract rates. This section is required for all LCDP proposals.
6) Platform Configuration Deliverables Proposals: This section will provide a detailed description of the proposed solutions that will fulfil the fixed-price deliverables stated within the Platform Configuration Deliverables section. Each proposal must explain how long it will take to execute the deliverable (where applicable) and the expectations required by NYSED for a successful delivery. LCDP proposals must include all three (3) deliverables. DMS proposals only need to include Deliverable #3. All proposals for Deliverable #3 must include a detailed list of deliverables that are included with the customer success plan.
7) Staff Augmentation Deliverables: This section will provide a description of the proposed staff augmentation solutions that will fulfill the Staff Augmentation section. This section must provide:
    a. Any proposed adjustments to the staffing process as described in the Staff Augmentation section. (Adjustments to the process will be considered at NYSED's sole discretion.)

b. Statistics on the Proposer's current talent pool availability, including the number of active candidates by role, staff augmentation average turnover period, and conversion rate from temporary staff to permanent staff.

This section is required for all proposals.

8) Sample Resumes: The Proposer must provide one resume per role from their current talent pool of staff augmentation candidates. The resume should have all personally identifying information removed from the resume. NYSED agrees that there will not be any expectation that these candidates will be available once the contract is awarded. We will use these resumes as a basis for evaluating the Proposer's ability to recruit qualified staff. This section is required for all proposals.
9) The proposer, along with any sub-contractors that provide in-scope technology platforms, must provide NYSED with their Service Organization Control (SOC) 2 Type 2 Report. NYSED agrees to keep this document highly confidential. The SOC 2 Type 2 Report may be provided through a separate encrypted communication channel from the RFP proposal. The proposal must include detailed instructions on how to request access to the Report. Access to the Report must be available within two business days of the submission of the proposal. These documents are required for all proposals.
10) Instructions to activate trial licenses for five (5) named users at NYSED for a three (3) month[8] or more trail period.

The competed Cost Proposal should be attached included and labeled **[Name of Bidder] - Cost Proposal – RFP #24-021 – [either LCDP or DMS].** Two templates for the Cost Proposals are provided with this RFP, one for DMS proposals and another for LCDP proposals. All cost proposals are required to use the provided templates. The template spreadsheets include an instruction tab. Those instructions must be followed.

M/WBE Documents

The original completed M/WBE Documents should be labeled **[Name of Bidder] - M/WBE Documents – RFP #24-021 – [either LCDP or DMS].** Please return the documents listed for the compliance method bidder has achieved:

Full Participation-No Request for Waiver

1. M/WBE Cover Letter, **Signatures Required**
2. **M/WBE 100** Utilization Plan
3. **M/WBE 102** Notice of Intent to Participate
4. **EEO 100** Staffing Plan

Partial Participation-Request for Partial Waiver

1. M/WBE Cover Letter, **Signatures Required**
2. **M/WBE 100** Utilization Plan
3. **M/WBE 102** Notice of Intent to Participate
4. **EEO 100** Staffing Plan
5. **M/WBE 101** Request for Waiver
6. **M/WBE 105** Contractor's Good Faith Efforts

[8] This should not be construed that the scoring period will take three (3) months.

No Participation-Request for Complete Waiver

1. M/WBE Cover Letter, **Signatures Required**
2. **EEO 100** Staffing Plan
3. **M/WBE 10**1 Request for Waiver
4. **M/WBE 105** Contractor's Good Faith Efforts

3.) Evaluation Criteria and Method of Award

This section begins with the criteria the agency will use to evaluate bids and closes with the "method of award," or how the contractor will be selected. This will be followed by various terms and conditions that reflect the specific needs of this project as well as New York State contract guidelines and requirements.

Criteria for Evaluating Bids

All eligible proposals received by the deadline will be reviewed using the following criteria and ratings. Applicants must ensure that all components of this application request have been addressed, all forms and assurances have been completed, and the original signatures are included as required.

An evaluation committee will complete a review of all proposals submitted. The committee will review each proposal based upon the submitted proposal and the requirements of the RFP only. Bidders should not assume that committee review members will be familiar with the current program or have any previous experience with the bidder. Appropriate description should be included to inform review committee members about the bidder's qualifications and capacity to perform all required deliverables.

The committee will review each proposal to determine compliance with the requirements described in the RFP. NYSED retains the right to determine whether any deviation from the requirements of this RFP is substantial in nature and may reject in whole or in part any and all proposals, waive minor irregularities and conduct discussions with all responsible bidders.

Proposals for LCDP and DMS will be scored and awarded separately. There will be two (2) different scoring criteria, based on which platform is being proposed. These criteria are as follows:

Criteria Type	Criteria	LCDP Proposal	DMS Proposal
Technical Criteria	Ability to meet LCDP Requirements	55	0
	Ability to meet DMS Requirements	0	60
	Ability to meet Platform Configuration Deliverables	5	5
	Ability to meet Cloud Infrastructure Services Deliverables	5	0
	Ability to meet staff augmentation requirements	5	5
Technical Criteria Points Total		**70**	**70**
Financial Criteria	LCDP Total Cost of Ownership	20	0
	DMS Total Cost of Ownership	0	20
	Staffing Costs	10	10
Financial Criteria Points Total		**30**	**30**
Total Points		**100**	**100**

Table 3: Scoring Criteria

The **financial portion** of the proposal represents 30 points of the overall score and will be awarded up to 30 points. This calculation will be computed by the Contract Administration Unit upon completion of the technical scoring by the technical review panel.

For each aspect of the submitted budget (total cost of ownership and staffing costs), the highest possible score (20 and 10 points, respectively) will be awarded to the proposal that reflects the lowest cost. The remaining proposals will be awarded points based on a calculation that computes the relative difference of each proposal against the lowest budget submitted and applies the resulting percentage to the maximum point value. The points for each section (total cost of ownership and staffing costs) will then be combined to obtain the total cost score.

NYSED reserves the right to request best and final offers. In the event NYSED exercises this right, all responsive bidders will be asked to provide a best and final offer. The Contract Administration Unit will recalculate the financial score.

Method of Award

The aggregate score of all the criteria listed will be calculated for each proposal received.

The contracts issued pursuant to this proposal will be awarded to the vendors whose aggregate technical and cost score is the highest among all the proposals rated. **If NYSED exercises the right to request best and final offers, the contract must be issued to the vendor with the highest aggregate technical and financial score that results from the best and final offer.**

One contract will be awarded to the proposer with the highest aggregate score for LCDP deliverables. Another contract will be awarded to the proposer with the highest aggregate score for DMS deliverables.

NYSED's Reservation of Rights

NYSED reserves the right to: (1) reject any or all proposals received in response to the RFP; (2) withdraw the RFP at any time, at the agency's sole discretion; (3) make an award under the RFP in whole or in part; (4) disqualify any bidder whose conduct and/or proposal fails to conform to the requirements of the RFP; (5) seek clarifications of proposals; (6) use proposal information obtained through site visits, management interviews and the state's investigation of a bidder's qualifications, experience, ability or financial standing, and any material or information submitted by the bidder in response to the agency's request for clarifying information in the course of evaluation and/or selection under the RFP; (7) prior to the bid opening, amend the RFP specifications to correct errors or oversights, or to supply additional information, as it becomes available; (8) prior to the bid opening, direct bidders to submit proposal modifications addressing subsequent RFP amendments; (9) change any of the scheduled dates; (10) waive any requirements that are not material; (11) negotiate with the successful bidder within the scope of the RFP in the best interests of the state; (12) conduct contract negotiations with the next responsible bidder, should the agency be unsuccessful in negotiating with the selected bidder; (13) utilize any and all ideas submitted in the proposals received; (14) unless otherwise specified in the solicitation, every offer is firm and not revocable for a period of 90 days from the bid opening; (15) require clarification at any time during the procurement process and/or require correction of arithmetic or other apparent errors for the purpose of assuring a full and complete understanding of an offerer's proposal and/or to determine an offerer's compliance with the requirements of the solicitation; (16) request demonstrations of the proposed platforms; (18) request best and final offers.

Post Selection Procedures

Upon selection, the successful bidder will receive a proposed contract from NYSED. The selected bidder may be given an opportunity to reduce its cost proposal in accordance with the agency's right to negotiate a final best price. The contents of this RFP, any subsequent correspondence during the proposal evaluation period, and such other stipulations as agreed upon may be made a part of the final contract prepared by NYSED. Successful bidders may be subject to audit and should ensure that adequate controls are in place to document the allowable activities and expenditure of State funds.

Debriefing Procedures

In accordance with section 163 of the NY State Finance Law, NYSED, upon request, must provide a debriefing to any unsuccessful bidder regarding the reasons their proposal was not selected for an award.

1. All unsuccessful bidders may request a debriefing within fifteen (15) calendar days of receiving notice from NYSED of non-award. Bidders may request a debriefing by submitting a written request to the Fiscal Contact person at rfp24-021@nysed.gov.

2. Upon receipt of a timely written request from the unsuccessful bidder, NYSED will schedule the debriefing to occur within a reasonable time following receipt of the request. Debriefings will be conducted in person, unless NYSED and the bidder mutually agree to utilize other means, including but not limited to telephone, video-conferencing or other types of electronic communication.

3. The debriefing will include: a) the reasons that the proposal submitted by the unsuccessful bidder was not selected for an award; b) the qualitative and quantitative analysis employed by NYSED in assessing the relative merits of the proposals; c) the application of the selection criteria to the unsuccessful bidder’s proposal; and d) when the debriefing is held after the final award, the reasons for the selection of the winning proposal. The debriefing will also provide, to the greatest extent practicable, general advice and guidance to the unsuccessful bidder concerning potential ways that their future proposals could be more responsive.

Contract Award Protest Procedures

Bidders who receive a notice of non-award or disqualification may protest the NYSED award decision subject to the following:

1. The protest must be in writing and must contain specific factual and/or legal allegations setting forth the basis on which the protesting party challenges the contract award by NYSED.

2. The protest must be filed within ten (10) business days of receipt of a debriefing or disqualification letter. The protest letter must be filed with the Contract Administration Unit by emailing: rfp24-021@nysed.gov.

3. The NYSED Contract Administration Unit (CAU) will convene a review team that will include at least one staff member from each of NYSED’s Office of Counsel, CAU, and the Program Office. The review team will review and consider the merits of the protest and will decide whether the protest is approved or denied. Counsel’s Office will provide the bidder with written notification of

the review team's decision within ten (10) business days of the receipt of the protest. The original protest and decision will be filed with OSC when the contract procurement record is submitted for approval and CAU will advise OSC that a protest was filed.

4. The NYSED Contract Administration Unit (CAU) may summarily deny a protest that fails to contain specific factual or legal allegations, or where the protest only raises issues of law that have already been decided by the courts.

Vendor Responsibility

State law requires that the award of state contracts be made to responsible vendors. Before an award is made to a not-for-profit entity, a for-profit entity, a private college or university or a public entity not exempted by the Office of the State Comptroller (OSC), NYSED must make an affirmative responsibility determination. The factors to be considered include legal authority to do business in New York State; integrity; capacity – both organizational and financial; and previous performance. Before an award of $100,000 or greater can be made to a covered entity, the entity will be required to complete and submit a Vendor Responsibility Questionnaire. School districts, Charter Schools, BOCES, public colleges and universities, public libraries, and the Research Foundation for SUNY and CUNY are some of the exempt entities. A complete list of exempt entities can be viewed at the Office of the State Comptroller's website.

NYSED recommends that vendors file the required Vendor Responsibility Questionnaire online via the New York State VendRep System. To enroll in and use the New York State VendRep System, see the VendRep System Instructions or go directly to the VendRep System on the Office of the State Comptroller's website.

Vendors must provide their New York State Vendor Identification Number when enrolling. To request assignment of a Vendor ID or for VendRep System assistance, contact the Office of the State Comptroller's Help Desk at 866-370-4672 or 518-408-4672 or by email at ITServiceDesk@osc.ny.gov.

Vendors opting to complete and submit a paper questionnaire can obtain the appropriate questionnaire from the VendRep website or may contact NYSED or the Office of the State Comptroller's Help Desk for a copy of the paper form.

Subcontractors:
For vendors using subcontractors, a Vendor Responsibility Questionnaire and a NYSED vendor responsibility review are required for a subcontractor where:

- The subcontractor is known at the time of the contract award.
- The subcontractor is not an entity that is exempt from reporting by OSC.
- The subcontract will equal or exceed $100,000 over the life of the contract.

Note: Bidders must acknowledge their method of filing their questionnaire by checking the appropriate box on the Response Sheet for Bids (5. Submission Documents).

Procurement Lobbying Law

Pursuant to State Finance Law §§139-j and 139-k, this solicitation includes and imposes certain restrictions on communications between the New York State Education Department ("NYSED") and an

Offerer/bidder during the procurement process. An Offerer/bidder is restricted from making contacts from the earliest notice of the solicitation through final award and approval of the Procurement Contract by NYSED and, if applicable, Office of the State Comptroller ("restricted period") to other than designated staff unless it is a contact that is included among certain statutory exceptions set forth in State Finance Law §139-j(3)(a). Designated staff, as of the date hereof, is identified below. NYSED employees are also required to obtain certain information when contacted during the restricted period and make a determination of the responsibility of the Offerer/bidder pursuant to these two statutes. Certain findings of non-responsibility can result in rejection for contract award and in the event of two findings within a four-year period, the Offerer/bidder is debarred from obtaining governmental Procurement Contracts. Further information about these requirements can be found at NYSED's Procurement Lobbying Law Policy Guidelines webpage.

Designated Contacts for NYSED
Program Office – **Gabrielle Fisher, Brian Waage**
Contract Administration Unit – **Jessica Hartjen**
M/WBE – **Brian Hackett**

Consultant Disclosure Legislation

Effective June 19, 2006, new reporting requirements became effective for State contractors, as the result of an amendment to State Finance Law §§ 8 and 163. As a result of these changes in law, State contractors will be required to disclose, by employment category, the number of persons employed to provide services under a contract for consulting services, the number of hours worked, and the amount paid to the contractor by the State as compensation for work performed by these employees. This will include information on any persons working under any subcontracts with the State contractor.

Chapter 10 of the Laws of 2006 expands the definition of contracts for consulting services to include any contract entered into by a State agency for analysis, evaluation, research, training, data processing, computer programming, engineering, environmental, health, and mental health services, accounting, auditing, paralegal, legal, or similar services.

To enable compliance with the law, State agencies must include in the Procurement Record submitted to OSC for new consultant contracts, the State Consultant Services Contractor's Planned Employment from Contract Start Date Through the End of the Contract Term (Form A). The completed form must include information for all employees providing service under the contract whether employed by the contractor or a subcontractor. Please note that the form captures the necessary planned employment information ***prospectively from the start date of the contract through the end of the contract term***.

Form A is available on OSC's website.

Please note that although this form is not required as part of the bid submission, NYSED encourages bidders to include it in their bid submission to expedite contract execution if the bidder is awarded the contract. Note also that only the form listed above is acceptable.
Chapter 10 of the Laws of 2006 mandates that State agencies must now require State contractors to **report annually** on the employment information described above, including work performed by subcontractors. The legislation mandates that the annual employment reports are to be submitted by the contractor to the contracting agency, to OSC and to the Department of Civil Service. State Consultant Services Contractor's Annual Employment Report (Form B) is to be used to report the information for all procurement contracts above $15,000. Please note that, in contrast to the information to be included on Form A, which is a one-time report of planned employment data for the entire term of

a consulting contract on a projected basis, ***Form B will be submitted each year the contract is in effect and will capture historical information, detailing actual employment data for the most recently concluded State fiscal year (April 1 – March 31).***

Form B is available on OSC's website.

For more information, please visit OSC Guide to Financial Operations.

Public Officer's Law Section 73

All bidders must comply with Public Officer's Law Section 73 (4)(a), as follows:

4. (a) No statewide elected official, state officer or employee, member of the legislature, legislative employee or political party chairman or firm or association of which such person is a member, or corporation, ten per centum or more of the stock of which is owned or controlled directly or indirectly by such person, shall (i) sell any goods or services having a value in excess of twenty-five dollars to any state agency, or (ii) contract for or provide such goods or services with or to any private entity where the power to contract, appoint or retain on behalf of such private entity is exercised, directly or indirectly, by a state agency or officer thereof, unless such goods or services are provided pursuant to an award or contract let after public notice and competitive bidding. This paragraph shall not apply to the publication of resolutions, advertisements or other legal propositions or notices in newspapers designated pursuant to law for such purpose and for which the rates are fixed pursuant to law.

(i) The term "state officer or employee" shall mean:
(i) heads of state departments and their deputies and assistants other than members of the board of regents of the university of the state of New York who receive no compensation or are compensated on a per diem basis,
(ii) officers and employees of statewide elected officials,
(iii) officers and employees of state departments, boards, bureaus, divisions, commissions, councils or other state agencies other than officers of such boards, commissions or councils who receive no compensation or are compensated on a per diem basis, and
(iv) members or directors of public authorities, other than multistate authorities, public benefit corporations and commissions at least one of whose members is appointed by the governor, who receive compensation other than on a per diem basis, and employees of such authorities, corporations and commissions.

Review Public Officer's Law Section 73.

NYSED Substitute Form W-9

Any payee/vendor/organization receiving Federal and/or State payments from NYSED must complete the NYSED Substitute Form W-9 if they are not yet registered in the Statewide Financial System centralized vendor file.

The NYS Education Department (NYSED) is using the NYSED Substitute Form W-9 to obtain certification of a vendor's Tax Identification Number in order to facilitate a vendor's registration with the SFS centralized vendor file and to ensure accuracy of information contained therein. We ask for the information on the NYSED Substitute Form W-9 to carry out the Internal Revenue laws of the United States.

RFP #24-021

Workers' Compensation Coverage and Debarment

New York State Workers' Compensation Law (WCL) has specific coverage requirements for businesses contracting with New York State and additional requirements which provide for the debarment of vendors that violate certain sections of WCL. The WCL requires, and has required since introduction of the law in 1922, the heads of all municipal and State entities to ensure that businesses have appropriate workers' compensation and disability benefits insurance coverage *prior* to issuing any permits or licenses, or *prior* to entering into contracts.

Workers' compensation requirements are covered by WCL Section 57, while disability benefits are covered by WCL Section 220(8). The Workers' Compensation Benefits clause in Appendix A – STANDARD CLAUSES FOR NEW YORK STATE CONTRACTS states that in accordance with Section 142 of the State Finance Law, a contract shall be void and of no force and effect unless the contractor provides and maintains coverage during the life of the contract for the benefit of such employees as are required to be covered by the provisions of the WCL.

Under provisions of the 2007 Workers' Compensation Reform Legislation (WCL Section 141-b), any person, or entity substantially owned by that person: subject to a final assessment of civil fines or penalties, subject to a stop-work order, or convicted of a misdemeanor for violation of Workers' Compensation laws Section 52 or 131, is barred from bidding on, or being awarded, any public work contract or subcontract with the State, any municipal corporation or public body for one year for each violation. The ban is five years for each felony conviction.

PROOF OF COVERAGE REQUIREMENTS

The Workers' Compensation Board has developed several forms to assist State contracting entities in ensuring that businesses have the appropriate workers' compensation and disability insurance coverage as required by Sections 57 and 220(8) of the WCL.

Please note – an ACORD form is not acceptable proof of New York State workers' compensation or disability benefits insurance coverage.

Proof of Workers' Compensation Coverage

To comply with coverage provisions of the WCL, the Workers' Compensation Board requires that a business seeking to enter into a State contract submit appropriate proof of coverage to the State contracting entity issuing the contract. For each new contract or contract renewal, the contracting entity must obtain ONE of the following forms from the contractor and submit to OSC to prove the contractor has appropriate workers' compensation insurance coverage:

- **Form C-105.2** – Certificate of Workers' Compensation Insurance issued by private insurance carriers, or **Form U-26.3** issued by the State Insurance Fund; or

- **Form SI-12**– Certificate of Workers' Compensation Self-Insurance; or **Form GSI-105.2** Certificate of Participation in Workers' Compensation Group Self-Insurance; or

- **CE-200**– Certificate of Attestation of Exemption from NYS Workers' Compensation and/or Disability Benefits Coverage.

Proof of Disability Benefits Coverage

To comply with coverage provisions of the WCL regarding disability benefits, the Workers' Compensation Board requires that a business seeking to enter into a State contract must submit appropriate proof of coverage to the State contracting entity issuing the contract. For each new contract or contract renewal, the contracting entity must obtain ONE of the following forms from the contractor and submit to OSC to prove the contractor has appropriate disability benefits insurance coverage:

- **Form DB-120.1** - Certificate of Disability Benefits Insurance; or
- **Form DB-155**- Certificate of Disability Benefits Self-Insurance; or
- **CE-200**– Certificate of Attestation of Exemption from New York State Workers' Compensation and/or Disability Benefits Coverage.

For additional information regarding workers' compensation and disability benefits requirements, please refer to the New York State Workers' Compensation Board website. Alternatively, questions relating to either workers' compensation or disability benefits coverage should be directed to the NYS Workers' Compensation Board, Bureau of Compliance at (518) 486-6307.

Please note that although these forms are not required as part of the bid submissions, NYSED encourages bidders to include them in their bid submission to expedite contract execution if the bidder is awarded the contract. Note also that only the forms listed above are acceptable.

Sales and Compensating Use Tax Certification (Tax Law, § 5-a)

Tax Law § 5-a requires contractors awarded State contracts for commodities or services valued at more than $100,000 over the full term of the contract to certify to the New York State Department of Taxation and Finance ("DTF") that they are registered to collect New York State and local sales and compensating use taxes, if they made sales delivered by any means to locations within New York State of tangible personal property or taxable services having a cumulative value in excess of $300,000, measured over a specific period of time. The registration requirement applies if the contractor made a cumulative total of more than $300,000 in sales during the four completed sales tax quarters which immediately precede the sales tax quarter in with the certification is made. Sales tax quarters are June – August, September – November, December – February, and March – May. In addition, contractors must certify to DTF that each affiliate and subcontractor of such contractor exceeding such sales threshold during a specified period is registered to collect New York State and local sales and compensating use taxes. Contractors must also certify to the procuring State entity that they filed the certification with the DTF and that it is correct and complete.

The selected bidder must file a properly completed Form ST-220-CA (with NYSED as the Contracting Agency) and Form ST-220-TD (with the DTF). These requirements must be met before a contract may take effect. Further information can be found at the New York State Department of Taxation and Finance's website. Forms are available through these links:

• ST-220 CA

• ST-220 TD

Please note that although these forms are not required as part of the bid submissions, NYSED encourages bidders to include them with their bid submissions to expedite contract execution if the bidder is awarded the contract.

RFP #24-021

4.) Assurances

The State of New York Agreement, Appendix A (Standard Clauses for all New York State Contracts), Appendix A-1 (Agency-Specific Clauses), and Appendix R (Data Security and Privacy Plan Provisions) **WILL BE INCLUDED** in the contract that results from this RFP. Vendors who are unable to complete or abide by these assurances should not respond to this request.

The documents listed below are included in **5.) Submission Documents**, which must be signed by the Chief Administrative Officer. Please review the terms and conditions. Certain documents will become part of the resulting contract that will be executed between the successful bidder and the NYS Education Department.

1. Non-Collusion Certification
2. MacBride Certification
3. Certification-Omnibus Procurement Act of 1992
4. Certification Regarding Lobbying; Debarment and Suspension; and Drug-Free Workplace Requirements
5. Offerer Disclosure of Prior Non-Responsibility Determinations
6. NYSED Substitute Form W-9 (If bidder is not yet registered in the SFS centralized vendor file.)
7. Iran Divestment Act Certification
8. Sexual Harassment Policy Certification
9. Certification Under Executive Order No. 16

M/WBE Documents **– (the forms below are included in 5.) Submission Documents)**
Please return the documents listed for the compliance method bidder has achieved:

Full Participation-No Request for Waiver
1. M/WBE Cover Letter
2. **M/WBE 100** Utilization Plan
3. **M/WBE 102** Notice of Intent to Participate
4. **EEO 100** Staffing Plan

Partial Participation-Request for Partial Waiver
1. M/WBE Cover Letter
2. **M/WBE 100** Utilization Plan
3. **M/WBE 102** Notice of Intent to Participate
4. **EEO 100** Staffing Plan
5. **M/WBE 101** Request for Waiver
6. **M/WBE 105** Contractor's Good Faith Efforts

No Participation-Request for Complete Waiver
1. M/WBE Cover Letter
2. **EEO 100** Staffing Plan
3. **M/WBE 101** Request for Waiver
4. **M/WBE 105** Contractor's Good Faith Efforts

STATE OF NEW YORK AGREEMENT

This AGREEMENT is hereby made by and between the People of the State of New York, acting through Dr. Betty A. Rosa, Commissioner of Education of the State of New York, party of the first part, hereinafter referred to as the (STATE) and the public or private agency (CONTRACTOR) identified on the face page hereof.

WITNESSETH:

WHEREAS, the STATE has the authority to regulate and provide funding for the establishment and operation of program services and desires to contract with skilled parties possessing the necessary resources to provide such services; and

WHEREAS, the CONTRACTOR is ready, willing and able to provide such program services and possesses or can make available all necessary qualified personnel, licenses, facilities and expertise to perform or have performed the services required pursuant to the terms of this AGREEMENT;

NOW THEREFORE, in consideration of the promises, responsibilities and covenants herein, the STATE and the CONTRACTOR agree as follows:

I. Conditions of Agreement

A. This AGREEMENT may consist of successive periods (PERIOD), as specified within the AGREEMENT or within a subsequent Modification Agreement(s) (Appendix X). Each additional or superseding PERIOD shall be on the forms specified by the particular State agency and shall be incorporated into this AGREEMENT.

B. Funding for the first PERIOD shall not exceed the funding amount specified on the face page hereof. Funding for each subsequent PERIOD, if any, shall not exceed the amount specified in the appropriate appendix for that PERIOD.

C. This AGREEMENT incorporates the face pages attached and all of the marked appendices identified on the face page hereof.

D. For each succeeding PERIOD of this AGREEMENT, the parties shall prepare new appendices, to the extent that any require modification, and a Modification Agreement (The attached Appendix X is the blank form to be used). Any terms of this AGREEMENT not modified shall remain in effect for each PERIOD of the AGREEMENT.

To modify the AGREEMENT within an existing PERIOD, the parties shall revise or complete the appropriate appendix form(s). Any change in the amount of consideration to be paid, or change in the term, is subject to the approval of the Office of the State Comptroller. Any other modifications shall be processed in accordance with agency guidelines as stated in Appendix A1.

E. The CONTRACTOR shall perform all services to the satisfaction of the STATE. The CONTRACTOR shall provide services and meet the program objectives summarized in the Program

Workplan (Appendix D) in accordance with: provisions of the AGREEMENT; relevant laws, rules and regulations, administrative and fiscal guidelines; and where applicable, operating certificates for facilities or licenses for an activity or program.

F. If the CONTRACTOR enters into subcontracts for the performance of work pursuant to this AGREEMENT, the CONTRACTOR shall take full responsibility for the acts and omissions of its subcontractors. Nothing in the subcontract shall impair the rights of the STATE under this AGREEMENT. No contractual relationship shall be deemed to exist between the subcontractor and the STATE.

G. Appendix A (Standard Clauses as required by the Attorney General for all State contracts) takes precedence over all other parts of the AGREEMENT.

II. Payment and Reporting

A. The CONTRACTOR, to be eligible for payment, shall submit to the STATE's designated payment office (identified in Appendix C) any appropriate documentation as required by the Payment and Reporting Schedule (Appendix C) and by agency fiscal guidelines, in a manner acceptable to the STATE.

B. The STATE shall make payments and any reconciliations in accordance with the Payment and Reporting Schedule (Appendix C). The STATE shall pay the CONTRACTOR, in consideration of contract services for a given PERIOD, a sum not to exceed the amount noted on the face page hereof or in the respective Appendix designating the payment amount for that given PERIOD. This sum shall not duplicate reimbursement from other sources for CONTRACTOR costs and services provided pursuant to this AGREEMENT.

C. The CONTRACTOR shall meet the audit requirements specified by the STATE.

III. Terminations

A. This AGREEMENT may be terminated at any time upon mutual written consent of the STATE and the CONTRACTOR.

B. The STATE may terminate the AGREEMENT immediately, upon written notice of termination to the CONTRACTOR, if the CONTRACTOR fails to comply with the terms and conditions of this AGREEMENT and/or with any laws, rules, regulations, policies or procedures affecting this AGREEMENT.

C. The STATE may also terminate this AGREEMENT for any reason in accordance with provisions set forth in Appendix A1.

D. Written notice of termination, where required, shall be sent by personal messenger service or by certified mail, return receipt requested. The termination shall be effective in accordance with the terms of the notice.

E. Upon receipt of notice of termination, the CONTRACTOR agrees to cancel, prior to the effective date of any prospective termination, as many outstanding obligations as possible, and agrees not to incur any new obligations after receipt of the notice without approval by the STATE.

F. The STATE shall be responsible for payment on claims pursuant to services provided and costs incurred pursuant to terms of the AGREEMENT. In no event shall the STATE be liable for expenses and obligations arising from the program(s) in this AGREEMENT after the termination date.

IV. Indemnification

A. The CONTRACTOR shall be solely responsible and answerable in damages for any and all accidents and/or injuries to persons (including death) or property arising out of or related to the services to be rendered by the CONTRACTOR or its subcontractors pursuant to this AGREEMENT. The CONTRACTOR shall indemnify and hold harmless the STATE and its officers and employees from claims, suits, actions, damages and costs of every nature arising out of the provision of services pursuant to this AGREEMENT.

B. The CONTRACTOR is an independent contractor and may neither hold itself out nor claim to be an officer, employee or subdivision of the STATE nor make any claim, demand or application to or for any right based upon any different status.

V. Property

Any equipment, furniture, supplies or other property purchased pursuant to this AGREEMENT is deemed to be the property of the STATE except as may otherwise be governed by Federal or State laws, rules or regulations, or as stated in Appendix Al.

VI. Safeguards for Services and Confidentiality

A. Services performed pursuant to this AGREEMENT are secular in nature and shall be performed in a manner that does not discriminate on the basis of religious belief or promote or discourage adherence to religion in general or particular religious beliefs.

B. Funds provided pursuant to this AGREEMENT shall not be used for any partisan political activity, or for activities that may influence legislation or the election or defeat of any candidate for public office.

C. Information relating to individuals who may receive services pursuant to this AGREEMENT shall be maintained and used only for the purposes intended under the contract and in conformity with applicable provisions of laws and regulations, or specified in Appendix A1.

Appendix A
STANDARD CLAUSES FOR NYS CONTRACTS

The parties to the attached contract, license, lease, amendment or other agreement of any kind (hereinafter, "the contract" or "this contract") agree to be bound by the following clauses which are hereby made a part of the contract (the word "Contractor" herein refers to any party other than the State, whether a contractor, licenser, licensee, lessor, lessee or any other party):

1. EXECUTORY CLAUSE. In accordance with Section 41 of the State Finance Law, the State shall have no liability under this contract to the Contractor or to anyone else beyond funds appropriated and available for this contract.

2. NON-ASSIGNMENT CLAUSE. In accordance with Section 138 of the State Finance Law, this contract may not be assigned by the Contractor or its right, title or interest therein assigned, transferred, conveyed, sublet or otherwise disposed of without the State's previous written consent, and attempts to do so are null and void. Notwithstanding the foregoing, such prior written consent of an assignment of a contract let pursuant to Article XI of the State Finance Law may be waived at the discretion of the contracting agency and with the concurrence of the State Comptroller where the original contract was subject to the State Comptroller's approval, where the assignment is due to a reorganization, merger or consolidation of the Contractor's business entity or enterprise. The State retains its right to approve an assignment and to require that any Contractor demonstrate its responsibility to do business with the State. The Contractor may, however, assign its right to receive payments without the State's prior written consent unless this contract concerns Certificates of Participation pursuant to Article 5-A of the State Finance Law.

3. COMPTROLLER'S APPROVAL. In accordance with Section 112 of the State Finance Law, if this contract exceeds $50,000 (or $75,000 for State University of New York or City University of New York contracts for goods, services, construction and printing, and $150,000 for State University Health Care Facilities) or if this is an amendment for any amount to a contract which, as so amended, exceeds said statutory amount, or if, by this contract, the State agrees to give something other than money when the value or reasonably estimated value of such consideration exceeds $25,000, it shall not be valid, effective or binding upon the State until it has been approved by the State Comptroller and filed in his office. Comptroller's approval of contracts let by the Office of General Services, either for itself or its customer agencies by the Office of General Services Business Services Center, is required when such contracts exceed $85,000. Comptroller's approval of contracts established as centralized contracts through the Office of General Services is required when such contracts exceed $125,000, and when a purchase order or other procurement transaction issued under such centralized contract exceeds $200,000.

4. WORKERS' COMPENSATION BENEFITS. In accordance with Section 142 of the State Finance Law, this contract shall be void and of no force and effect unless the Contractor shall provide and maintain coverage during the life of this contract for the benefit of such employees as are required to be covered by the provisions of the Workers' Compensation Law.

5. NON-DISCRIMINATION REQUIREMENTS. To the extent required by Article 15 of the Executive Law (also known as the Human Rights Law) and all other State and Federal statutory and constitutional non-discrimination provisions, the Contractor will not discriminate against any employee or applicant for employment, nor subject any individual to harassment, because of age, race, creed, color, national origin, citizenship or immigration status, sexual orientation, gender identity or expression, military status, sex, disability, predisposing genetic characteristics, familial status, marital status, or domestic violence victim status or because the individual has opposed any practices forbidden under the Human Rights Law or has filed a complaint, testified, or assisted in any proceeding under the Human Rights Law. Furthermore, in accordance with Section 220-e of the Labor Law, if this is a contract for the construction, alteration or repair of any public building or public work or for the manufacture, sale or distribution of materials, equipment or supplies, and to the extent that this contract shall be performed within the State of

New York, Contractor agrees that neither it nor its subcontractors shall, by reason of race, creed, color, disability, sex, or national origin: (a) discriminate in hiring against any New York State citizen who is qualified and available to perform the work; or (b) discriminate against or intimidate any employee hired for the performance of work under this contract. If this is a building service contract as defined in Section 230 of the Labor Law, then, in accordance with Section 239 thereof, Contractor agrees that neither it nor its subcontractors shall by reason of race, creed, color, national origin, age, sex or disability: (a) discriminate in hiring against any New York State citizen who is qualified and available to perform the work; or (b) discriminate against or intimidate any employee hired for the performance of work under this contract. Contractor is subject to fines of $50.00 per person per day for any violation of Section 220-e or Section 239 as well as possible termination of this contract and forfeiture of all moneys due hereunder for a second or subsequent violation.

6. WAGE AND HOURS PROVISIONS. If this is a public work contract covered by Article 8 of the Labor Law or a building service contract covered by Article 9 thereof, neither Contractor's employees nor the employees of its subcontractors may be required or permitted to work more than the number of hours or days stated in said statutes, except as otherwise provided in the Labor Law and as set forth in prevailing wage and supplement schedules issued by the State Labor Department. Furthermore, Contractor and its subcontractors must pay at least the prevailing wage rate and pay or provide the prevailing supplements, including the premium rates for overtime pay, as determined by the State Labor Department in accordance with the Labor Law. Additionally, effective April 28, 2008, if this is a public work contract covered by Article 8 of the Labor Law, the Contractor understands and agrees that the filing of payrolls in a manner consistent with Subdivision 3-a of Section 220 of the Labor Law shall be a condition precedent to payment by the State of any State approved sums due and owing for work done upon the project.

7. NON-COLLUSIVE BIDDING CERTIFICATION. In accordance with Section 139-d of the State Finance Law, if this contract was awarded based upon the submission of bids, Contractor affirms, under penalty of perjury, that its bid was arrived at independently and without collusion aimed at restricting competition. Contractor further affirms that, at the time Contractor submitted its bid, an authorized and responsible person executed and delivered to the State a non-collusive bidding certification on Contractor's behalf.

8. INTERNATIONAL BOYCOTT PROHIBITION. In accordance with Section 220-f of the Labor Law and Section 139-h of the State Finance Law, if this contract exceeds $5,000, the Contractor agrees, as a material condition of the contract, that neither the Contractor nor any substantially owned or affiliated person, firm, partnership or corporation has participated, is participating, or shall participate in an international boycott in violation of the federal Export Administration Act of 1979 (50 USC App. Sections 2401 et seq.) or regulations thereunder. If such Contractor, or any of the aforesaid affiliates of Contractor, is convicted or is otherwise found to have violated said laws or regulations upon the final determination of the United States Commerce Department or any other appropriate agency of the United States subsequent to the contract's execution, such contract, amendment or modification thereto shall be rendered forfeit and void. The Contractor shall so notify the State Comptroller within five (5) business days of such conviction, determination or disposition of appeal (2 NYCRR § 105.4).

9. SET-OFF RIGHTS. The State shall have all of its common law, equitable and statutory rights of set-off. These rights shall include, but not be limited to, the State's option to withhold for the purposes of set-off any moneys due to the Contractor under this contract up to any amounts due and owing to the State with regard to this contract, any other contract with any State department or agency, including any contract for a term commencing prior to the term of this contract, plus any amounts due and owing to the State for any other reason including, without limitation, tax delinquencies, fee delinquencies or monetary penalties relative thereto. The State shall exercise its set-off rights in accordance with normal State practices including, in cases of set-

off pursuant to an audit, the finalization of such audit by the State agency, its representatives, or the State Comptroller.

10. RECORDS. The Contractor shall establish and maintain complete and accurate books, records, documents, accounts and other evidence directly pertinent to performance under this contract (hereinafter, collectively, the "Records"). The Records must be kept for the balance of the calendar year in which they were made and for six (6) additional years thereafter. The State Comptroller, the Attorney General and any other person or entity authorized to conduct an examination, as well as the agency or agencies involved in this contract, shall have access to the Records during normal business hours at an office of the Contractor within the State of New York or, if no such office is available, at a mutually agreeable and reasonable venue within the State, for the term specified above for the purposes of inspection, auditing and copying. The State shall take reasonable steps to protect from public disclosure any of the Records which are exempt from disclosure under Section 87 of the Public Officers Law (the "Statute") provided that: (i) the Contractor shall timely inform an appropriate State official, in writing, that said records should not be disclosed; and (ii) said records shall be sufficiently identified; and (iii) designation of said records as exempt under the Statute is reasonable. Nothing contained herein shall diminish, or in any way adversely affect, the State's right to discovery in any pending or future litigation.

11. IDENTIFYING INFORMATION AND PRIVACY NOTIFICATION. (a) Identification Number(s). Every invoice or New York State Claim for Payment submitted to a New York State agency by a payee, for payment for the sale of goods or services or for transactions (e.g., leases, easements, licenses, etc.) related to real or personal property must include the payee's identification number. The number is any or all of the following: (i) the payee's Federal employer identification number, (ii) the payee's Federal social security number, and/or (iii) the payee's Vendor Identification Number assigned by the Statewide Financial System. Failure to include such number or numbers may delay payment. Where the payee does not have such number or numbers, the payee, on its invoice or Claim for Payment, must give the reason or reasons why the payee does not have such number or numbers.

(b) Privacy Notification. (1) The authority to request the above personal information from a seller of goods or services or a lessor of real or personal property, and the authority to maintain such information, is found in Section 5 of the State Tax Law. Disclosure of this information by the seller or lessor to the State is mandatory. The principal purpose for which the information is collected is to enable the State to identify individuals, businesses and others who have been delinquent in filing tax returns or may have understated their tax liabilities and to generally identify persons affected by the taxes administered by the Commissioner of Taxation and Finance. The information will be used for tax administration purposes and for any other purpose authorized by law. (2) The personal information is requested by the purchasing unit of the agency contracting to purchase the goods or services or lease the real or personal property covered by this contract or lease. The information is maintained in the Statewide Financial System by the Vendor Management Unit within the Bureau of State Expenditures, Office of the State Comptroller, 110 State Street, Albany, New York 12236.

12. EQUAL EMPLOYMENT OPPORTUNITIES FOR MINORITIES AND WOMEN. In accordance with Section 312 of the Executive Law and 5 NYCRR Part 143, if this contract is: (i) a written agreement or purchase order instrument, providing for a total expenditure in excess of $25,000.00, whereby a contracting agency is committed to expend or does expend funds in return for labor, services, supplies, equipment, materials or any combination of the foregoing, to be performed for, or rendered or furnished to the contracting agency; or (ii) a written agreement in excess of $100,000.00 whereby a contracting agency is committed to expend or does expend funds for the acquisition, construction, demolition, replacement, major repair or renovation of real property and improvements thereon; or (iii) a written agreement in excess of $100,000.00 whereby the owner of a State assisted housing project is committed to expend or does expend funds for the acquisition, construction, demolition,

replacement, major repair or renovation of real property and improvements thereon for such project, then the following shall apply and by signing this agreement the Contractor certifies and affirms that it is Contractor's equal employment opportunity policy that:

(a) The Contractor will not discriminate against employees or applicants for employment because of race, creed, color, national origin, sex, age, disability or marital status, shall make and document its conscientious and active efforts to employ and utilize minority group members and women in its work force on State contracts and will undertake or continue existing programs of affirmative action to ensure that minority group members and women are afforded equal employment opportunities without discrimination. Affirmative action shall mean recruitment, employment, job assignment, promotion, upgradings, demotion, transfer, layoff, or termination and rates of pay or other forms of compensation;

(b) at the request of the contracting agency, the Contractor shall request each employment agency, labor union, or authorized representative of workers with which it has a collective bargaining or other agreement or understanding, to furnish a written statement that such employment agency, labor union or representative will not discriminate on the basis of race, creed, color, national origin, sex, age, disability or marital status and that such union or representative will affirmatively cooperate in the implementation of the Contractor's obligations herein; and

(c) the Contractor shall state, in all solicitations or advertisements for employees, that, in the performance of the State contract, all qualified applicants will be afforded equal employment opportunities without discrimination because of race, creed, color, national origin, sex, age, disability or marital status.

Contractor will include the provisions of "(a), (b) and (c)" above, in every subcontract over $25,000.00 for the construction, demolition, replacement, major repair, renovation, planning or design of real property and improvements thereon (the "Work") except where the Work is for the beneficial use of the Contractor. Section 312 does not apply to: (i) work, goods or services unrelated to this contract; or (ii) employment outside New York State. The State shall consider compliance by a contractor or subcontractor with the requirements of any federal law concerning equal employment opportunity which effectuates the purpose of this clause. The contracting agency shall determine whether the imposition of the requirements of the provisions hereof duplicate or conflict with any such federal law and if such duplication or conflict exists, the contracting agency shall waive the applicability of Section 312 to the extent of such duplication or conflict. Contractor will comply with all duly promulgated and lawful rules and regulations of the Department of Economic Development's Division of Minority and Women's Business Development pertaining hereto.

13. CONFLICTING TERMS. In the event of a conflict between the terms of the contract (including any and all attachments thereto and amendments thereof) and the terms of this Appendix A, the terms of this Appendix A shall control.

14. GOVERNING LAW. This contract shall be governed by the laws of the State of New York except where the Federal supremacy clause requires otherwise.

15. LATE PAYMENT. Timeliness of payment and any interest to be paid to Contractor for late payment shall be governed by Article 11-A of the State Finance Law to the extent required by law.

16. NO ARBITRATION. Disputes involving this contract, including the breach or alleged breach thereof, may not be submitted to binding arbitration (except where statutorily authorized), but must, instead, be heard in a court of competent jurisdiction of the State of New York.

17. SERVICE OF PROCESS. In addition to the methods of service allowed by the State Civil Practice Law & Rules ("CPLR"), Contractor hereby consents to service of process upon it by registered or certified mail, return receipt requested. Service hereunder shall be complete upon Contractor's actual receipt of process or upon the State's receipt of the return thereof by the United States Postal Service as refused or

undeliverable. Contractor must promptly notify the State, in writing, of each and every change of address to which service of process can be made. Service by the State to the last known address shall be sufficient. Contractor will have thirty (30) calendar days after service hereunder is complete in which to respond.

18. PROHIBITION ON PURCHASE OF TROPICAL HARDWOODS. The Contractor certifies and warrants that all wood products to be used under this contract award will be in accordance with, but not limited to, the specifications and provisions of Section 165 of the State Finance Law, (Use of Tropical Hardwoods) which prohibits purchase and use of tropical hardwoods, unless specifically exempted, by the State or any governmental agency or political subdivision or public benefit corporation. Qualification for an exemption under this law will be the responsibility of the contractor to establish to meet with the approval of the State.

In addition, when any portion of this contract involving the use of woods, whether supply or installation, is to be performed by any subcontractor, the prime Contractor will indicate and certify in the submitted bid proposal that the subcontractor has been informed and is in compliance with specifications and provisions regarding use of tropical hardwoods as detailed in § 165 State Finance Law. Any such use must meet with the approval of the State; otherwise, the bid may not be considered responsive. Under bidder certifications, proof of qualification for exemption will be the responsibility of the Contractor to meet with the approval of the State.

19. MACBRIDE FAIR EMPLOYMENT PRINCIPLES. In accordance with the MacBride Fair Employment Principles (Chapter 807 of the Laws of 1992), the Contractor hereby stipulates that the Contractor either (a) has no business operations in Northern Ireland, or (b) shall take lawful steps in good faith to conduct any business operations in Northern Ireland in accordance with the MacBride Fair Employment Principles (as described in Section 165 of the New York State Finance Law), and shall permit independent monitoring of compliance with such principles.

20. OMNIBUS PROCUREMENT ACT OF 1992. It is the policy of New York State to maximize opportunities for the participation of New York State business enterprises, including minority- and women-owned business enterprises as bidders, subcontractors and suppliers on its procurement contracts.

Information on the availability of New York State subcontractors and suppliers is available from:

NYS Department of Economic Development
Division for Small Business and Technology Development
625 Broadway
Albany, New York 12245
Telephone: 518-292-5100

A directory of certified minority- and women-owned business enterprises is available from:

NYS Department of Economic Development
Division of Minority and Women's Business Development
633 Third Avenue 33rd Floor
New York, NY 10017
646-846-7364
email: mwbebusinessdev@esd.ny.gov
NYS M/WBE Directory

The Omnibus Procurement Act of 1992 (Chapter 844 of the Laws of 1992, codified in State Finance Law § 139-i and Public Authorities Law § 2879(3)(n)–(p)) requires that by signing this bid proposal or contract, as applicable, Contractors certify that whenever the total bid amount is greater than $1 million:

(a) The Contractor has made reasonable efforts to encourage the participation of New York State Business Enterprises as suppliers and subcontractors, including certified minority- and women-owned business enterprises, on this project, and has retained the documentation of these efforts to be provided upon request to the State;

(b) The Contractor has complied with the Federal Equal Opportunity Act of 1972 (P.L. 92-261), as amended;

(c) The Contractor agrees to make reasonable efforts to provide notification to New York State residents of employment opportunities on this project through listing any such positions with the Job Service Division of the New York State Department of Labor, or providing such notification in such manner as is consistent with existing collective bargaining contracts or agreements. The Contractor agrees to document these efforts and to provide said documentation to the State upon request; and

(d) The Contractor acknowledges notice that the State may seek to obtain offset credits from foreign countries as a result of this contract and agrees to cooperate with the State in these efforts.

21. RECIPROCITY AND SANCTIONS PROVISIONS. Bidders are hereby notified that if their principal place of business is located in a country, nation, province, state or political subdivision that penalizes New York State vendors, and if the goods or services they offer will be substantially produced or performed outside New York State, the Omnibus Procurement Act 1994 and 2000 amendments (Chapter 684 and Chapter 383, respectively, codified in State Finance Law § 165(6) and Public Authorities Law § 2879(5)) require that they be denied contracts which they would otherwise obtain. NOTE: As of May 2023, the list of discriminatory jurisdictions subject to this provision includes the states of South Carolina, Alaska, West Virginia, Wyoming, Louisiana and Hawaii.

22. COMPLIANCE WITH BREACH NOTIFICATION AND DATA SECURITY LAWS. Contractor shall comply with the provisions of the New York State Information Security Breach and Notification Act (General Business Law §§ 899-aa and 899-bb and State Technology Law § 208).

23. COMPLIANCE WITH CONSULTANT DISCLOSURE LAW. If this is a contract for consulting services, defined for purposes of this requirement to include analysis, evaluation, research, training, data processing, computer programming, engineering, environmental, health, and mental health services, accounting, auditing, paralegal, legal or similar services, then, in accordance with Section 163 (4)(g) of the State Finance Law (as amended by Chapter 10 of the Laws of 2006), the Contractor shall timely, accurately and properly comply with the requirement to submit an annual employment report for the contract to the agency that awarded the contract, the Department of Civil Service and the State Comptroller.

24. PROCUREMENT LOBBYING. To the extent this agreement is a "procurement contract" as defined by State Finance Law §§ 139-j and 139-k, by signing this agreement the contractor certifies and affirms that all disclosures made in accordance with State Finance Law §§ 139-j and 139-k are complete, true and accurate. In the event such certification is found to be intentionally false or intentionally incomplete, the State may terminate the agreement by providing written notification to the Contractor in accordance with the terms of the agreement.

25. CERTIFICATION OF REGISTRATION TO COLLECT SALES AND COMPENSATING USE TAX BY CERTAIN STATE CONTRACTORS, AFFILIATES AND SUBCONTRACTORS.
To the extent this agreement is a contract as defined by Tax Law § 5-a, if the contractor fails to make the certification required by Tax Law § 5-a or if during the term of the contract, the Department of Taxation and Finance or the covered agency, as defined by Tax Law § 5-a, discovers that the certification, made under penalty of perjury, is false, then such failure to file or false certification shall be a material breach of this contract and this contract may be terminated, by providing written notification to the Contractor in accordance with the terms of the agreement, if the covered agency determines that such action is in the best interest of the State.

26. IRAN DIVESTMENT ACT. By entering into this Agreement, Contractor certifies in accordance with State Finance Law § 165-a that it is not on the "Entities Determined to be Non-Responsive Bidders/Offerers pursuant to the New York State Iran Divestment Act of 2012" ("Prohibited Entities List").

Contractor further certifies that it will not utilize on this Contract any subcontractor that is identified on the Prohibited Entities List. Contractor agrees that should it seek to renew or extend this Contract, it must provide the same certification at

the time the Contract is renewed or extended. Contractor also agrees that any proposed Assignee of this Contract will be required to certify that it is not on the Prohibited Entities List before the contract assignment will be approved by the State.

During the term of the Contract, should the state agency receive information that a person (as defined in State Finance Law § 165-a) is in violation of the above-referenced certifications, the state agency will review such information and offer the person an opportunity to respond. If the person fails to demonstrate that it has ceased its engagement in the investment activity which is in violation of the Act within 90 days after the determination of such violation, then the state agency shall take such action as may be appropriate and provided for by law, rule, or contract, including, but not limited to, imposing sanctions, seeking compliance, recovering damages, or declaring the Contractor in default.

The state agency reserves the right to reject any bid, request for assignment, renewal or extension for an entity that appears on the Prohibited Entities List prior to the award, assignment, renewal or extension of a contract, and to pursue a responsibility review with respect to any entity that is awarded a contract and appears on the Prohibited Entities list after contract award.

27. ADMISSIBILITY OF REPRODUCTION OF CONTRACT. Notwithstanding the best evidence rule or any other legal principle or rule of evidence to the contrary, the Contractor acknowledges and agrees that it waives any and all objections to the admissibility into evidence at any court proceeding or to the use at any examination before trial of an electronic reproduction of this contract, in the form approved by the State Comptroller, if such approval was required, regardless of whether the original of said contract is in existence.

(June 2023)

APPENDIX A-1
AGENCY-SPECIFIC CLAUSES

Payment and Reporting

A. In the event that Contractor shall receive, from any source whatsoever, sums the payment of which is in consideration for the same costs and services provided to the State, the monetary obligation of the State hereunder shall be reduced by an equivalent amount provided, however, that nothing contained herein shall require such reimbursement where additional similar services are provided and no duplicative payments are received.

B. For each individual for whom costs are claimed under this agreement, the contractor warrants that the individual has been classified as an employee or as an independent contractor in accordance with 2 NYCRR 315 and all applicable laws including, but not limited to, the Internal Revenue Code, the New York Retirement and Social Security Law, the New York Education Law, the New York Labor Law, and the New York Tax Law. Furthermore, the contractor warrants that all project funds allocated to the proposed budget for Employee Benefits, represent costs for employees of the contractor only and that such funds will not be expended on any individual classified as an independent contractor.

Terminations

A. The State may terminate this Agreement without cause by thirty (30) days prior written notice. In the event of such termination, the parties will adjust the accounts due and the Contractor will undertake no additional expenditures not already required. Upon any such termination, the parties shall endeavor in an orderly manner to wind down activities hereunder.

B. SED reserves the right to terminate this Agreement in the event it is found that the certification by the Contractor in accordance with New York State Finance Law §139-k was intentionally false or intentionally incomplete. Upon such finding, SED may exercise its termination right by providing written notification to the Contractor in accordance with the written notification terms of this Agreement.

Responsibility Provisions

A. General Responsibility Language
The Contractor shall at all times during the Contract term remain responsible. The Contractor agrees, if requested by the Commissioner of Education or his or her designee, to present evidence of its continuing legal authority to do business in New York State, integrity, experience, ability, prior performance, and organizational and financial capacity.

B. Suspension of Work (for Non-Responsibility)
The Commissioner of Education or his or her designee, in his or her sole discretion, reserves the right to suspend any or all activities under this Contract, at any time, when he or she discovers information that calls into question the responsibility of the Contractor. In the event of such suspension, the Contractor will be given written notice outlining the particulars of such suspension. Upon issuance of such notice, the Contractor must comply with the terms of the suspension order. Contract activity may resume at such time as the Commissioner of Education or his or her designee issues a written notice authorizing a resumption of performance under the Contract.

C. Termination (for Non-Responsibility)
Upon written notice to the Contractor, and a reasonable opportunity to be heard with appropriate SED officials or staff, the Contract may be terminated by the Commissioner of Education or his or her designee at the Contractor's expense where the Contractor is determined by the Commissioner of Education or his or her designee to be non-responsible. In such event, the Commissioner or his or her designee may complete the contractual requirements in any manner he or she may deem advisable and pursue available legal or equitable remedies for breach.

Property

A. The Contractor shall maintain a complete inventory of all realty, equipment and other non-expendable assets including, but not limited to, books, paintings, artifacts, rare coins, antiques and other collectible items purchased, improved or developed under this agreement.

Inventories for non-expendable assets must be submitted with the final expenditure report. In addition to or as part of whatever rights the State may have with respect to the inspection of the Contractor, the State shall have the right to inspect the inventory without notice to the Contractor.

The Contractor shall not at any time sell, trade, convey or otherwise dispose of any non-expendable assets having a market value in excess of Two Thousand Dollars ($2,000) at the time of the desired disposition without the express permission of the State. The Contractor may seek permission in writing by certified mail to the State.

The Contractor shall not at any time use or allow to be used any non-expendable assets in a manner inconsistent with the purposes of this agreement.

B. If the Contractor wishes to continue to use any of the non-expendable assets purchased with the funds available under this agreement upon the termination of this agreement, it shall request permission from the State in writing for such continued use within twenty-five (25) days of the termination of this agreement. The Contractor's request shall itemize the non-expendable assets for which continued use is sought. The State may accept, reject or accept in part such request. If the request for continued use is allowed to any degree, it shall be conditioned upon the fact that said equipment shall continue to be used in accordance with the purposes of this agreement.

If after the State grants permission to the Contractor for "continued use" as set forth above the non-expendable assets are not used in accordance with the purposes of this agreement, the State in its discretion may elect to take title to such assets and may assert its right to possession upon thirty (30) days prior written notice by certified mail to the Contractor. The State upon obtaining such non-expendable assets may arrange for their further use in the public interest as it in its discretion may decide.

C. Upon termination of this agreement, the State in its discretion may elect to take title and may assert its right to possession of any non-expendable assets upon thirty (30) days prior written notice by certified mail to the Contractor. The State's option to elect to take title shall be triggered by the termination of this agreement or by the State's rejection of continued use of non-expendable assets by the Contractor as set forth herein. The State upon obtaining such non-expendable assets may arrange for their further use in the public interest as it in its discretion may decide.

D. The terms and conditions set forth herein regarding non-expendable assets shall survive the expiration or termination, for whatever reason, of this agreement.

Safeguards for Services and Confidentiality

A. Any copyrightable work produced pursuant to said agreement shall be the sole and exclusive property of the New York State Education Department. The material prepared under the terms of this agreement by the Contractor shall be prepared by the Contractor in a form so that it will be ready for copyright in the name of the New York State Education Department. Should the Contractor use the services of consultants or other organizations or individuals who are not regular employees of the Contractor, the Contractor and such organization or individual shall, prior to the performance of any work pursuant to this agreement, enter into a written agreement, duly executed, which shall set forth the services to be provided by such organization or individual and the consideration therefor. Such agreement shall provide that any copyrightable work produced pursuant to said agreement shall be the sole and exclusive property of the New York State Education Department and that such work shall be prepared in a form ready for copyright by the New York State Education Department. A copy of such agreement shall be provided to the State.

B. Required Web Accessibility of Delivered Documents and Applications. If applicable, all documentation, applications development, or programming delivered pursuant to the contract or procurement, will comply with New York State Education Department IT Policy NYSED-WEBACC-001, Web Accessibility Policy, which requires that documents, web-based information and applications are accessible to persons with disabilities. All delivered documentation and applications must conform to NYSED-WEBACC-001 as determined by quality assurance testing. Such quality assurance testing will be conducted by NYSED employee or contractor, and the results of such testing must be satisfactory to NYSED before documents and applications will be considered a qualified deliverable under the contract or procurement.

C. All reports of research, studies, publications, workshops, announcements, and other activities funded as a result of this proposal will acknowledge the support provided by the State of New York.

D. This agreement cannot be modified, amended, or otherwise changed except by a writing signed by all parties to this contract.

E. No failure to assert any rights or remedies available to the State under this agreement shall be considered a waiver of such right or remedy or any other right or remedy unless such waiver is contained in a writing signed by the party alleged to have waived its right or remedy.

F. Expenses for travel, lodging, and subsistence shall be reimbursed at the per diem rate in effect at the time for New York State Management/Confidential employees.

G. No fees shall be charged by the Contractor for training provided under this agreement.

H. Partisan Political Activity and Lobbying. Funds provided pursuant to this Agreement shall not be used for any partisan political activity or for activities that may influence legislation or the election or defeat of any candidate for public office.

I. Nothing herein shall require the State to adopt the curriculum developed pursuant to this agreement.

J. This agreement, including all appendices, is, upon signature of the parties and the approval of the Attorney General and the State Comptroller, a legally enforceable contract. Therefore, a signature on behalf of the Contractor will bind the Contractor to all the terms and conditions stated therein.

The parties to this agreement intend the foregoing writing to be the final, complete, and exclusive expression of all the terms of their agreement.

Certifications

A. Contractor certifies that it has met the disclosure requirements of State Finance Law §139-k and that all information provided to the State Education Department with respect to State Finance Law §139-k is complete, true and accurate.

B. Contractor certifies that it has not knowingly and willfully violated the prohibitions against impermissible contacts found in State Finance Law §139-j.

C. Contractor certifies that no governmental entity has made a finding of non-responsibility regarding the Contractor in the previous four years.

D. Contractor certifies that no governmental entity or other governmental agency has terminated or withheld a procurement contract with the Contractor due to the intentional provision of false or incomplete information.

E. Contractor affirms that it understands and agrees to comply with the procedures of the STATE relative to permissible contacts as required by State Finance Law §139-j (3) and §139-j (6)(b).

F. Contractor certifies that it is in compliance with NYS Public Officers Law, including but not limited to, §73(4)(a).

Notices

Any written notice or delivery under any provision of this AGREEMENT shall be deemed to have been properly made if sent by certified mail, return receipt requested to the address(es) set forth in this Agreement, except as such address(es) may be changed by notice in writing. Notice shall be considered to have been provided as of the date of receipt of the notice by the receiving party.

Miscellaneous

A. Contractor shall comply with the provisions of the New York State Information Security Breach and Notification Act (General Business Law Section 899-aa; State Technology Law Section 208). Contractor shall be liable for the costs associated with such breach if caused by Contractor's negligent or willful acts or omissions, or the negligent or willful acts or omissions of Contractor's agents, officers, employees or subcontractors.

B. If required by the Office of State Comptroller ("OSC") Bulletin G-226 and State Finance Law §§ 8 and 163, Contractor agrees to submit an initial planned employment data report on Form A and an annual employment report on Form B. State will furnish Form A and Form B to Contractor if required.

C. The initial planned employment report must be submitted at the time of approval of this Agreement. The annual employment report on Form B is due by May 15th of each year and covers actual employment data performed during the prior period of April 1st to March 31st. Copies of the report will be submitted to the NYS Education Department, OSC and the NYS Department of Civil Service at the addresses below.

By mail: NYS Office of the State Comptroller
Bureau of Contracts
110 State Street, 11th Floor
Albany, NY 12236
Attn: Consultant Reporting
By fax: (518) 474-8030 or (518) 473-8808

Reports to DCS are to be transmitted as follows:

By mail: NYS Department of Civil Service
Office of Counsel
Alfred E. Smith Office Building
Albany, NY 12239

Reports to NYSED are to be transmitted as follows:

By mail: NYS Education Department
Contract Administration Unit
Room 505 W EB
Albany, NY 12234
By fax: (518) 408-1716

C. Consultant Staff Changes. If this is a contract for consulting services, Contractor will maintain continuity of the consultant team staff throughout the course of the contract. All changes in staff will be subject to STATE approval. The replacement consultant(s) with comparable skills will be provided at the same or lower hourly rate.

D. Order of Precedence. In the event of any discrepancy, disagreement, conflict or ambiguity between the various documents, attachments and appendices comprising this contract, they shall be given preference in the following order to resolve any such discrepancy, disagreement, conflict or ambiguity:

1. Appendix A - Standard Clauses for all State Contracts
2. State of New York Agreement
3. Appendix A-1 - Agency Specific Clauses
4. Appendix X - Sample Modification Agreement Form (where applicable)
5. Appendix A-3 - Minority/Women-owned Business Enterprise Requirements (where applicable)
6. Appendix B - Budget
7. Appendix C - Payment and Reporting Schedule
8. Appendix R – Security and Privacy Mandates (where applicable)
9. Appendix D - Program Work Plan

Revised 5/23/22

Appendix R
NEW YORK STATE EDUCATION DEPARTMENT'S
DATA PRIVACY APPENDIX FOR CONFIDENTIAL DATA
ARTICLE I: DEFINITIONS

As used in this Data Privacy Appendix("DPA"), the following terms shall have the following meanings:

1. **Access**: The ability to view or otherwise obtain, but not copy or save, Personal Information arising from the on-site use of an information system or a personal meeting.
2. **Breach:** The unauthorized Access, acquisition, Disclosure or use of Personal Information in a manner not permitted by New York State and federal laws, rules and regulations, or in a manner that compromises its security or privacy, or by or to a person not authorized to acquire, Access, use, or receive it, or a Breach of Contractor's security that leads to the accidental or unlawful alteration, destruction, loss of, Access to or Disclosure of Personal Information.
3. **Disclose or Disclosure**: The intentional or unintentional communication, release, or transfer of Personal Information by any means, including oral, written, or electronic.
4. **Encrypt or Encryption**: The use of an algorithmic process to transform Personal Information into an unusable, unreadable, or indecipherable form in which there is a low probability of assigning meaning without use of a confidential process or key.
5. **NIST Cybersecurity Framework**: The U.S. Department of Commerce National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity Version 1.1.
6. **Personal Information:** Information concerning a natural person which, because of name, number, personal mark, or another identifier, can be used to identify such natural person.
7. **Release:** Shall have the same meaning as Disclose.
8. **Services:** Services provided by Contractor pursuant to this contract with the NYS Education Department to which this DPA is attached and incorporated.
9. **Subcontractor:** Contractor's non-employee agents, consultants, volunteers including student interns, and/or any natural person or entity funded through this Contract who is engaged in the provision of Services pursuant to an agreement with or at the direction of the Contractor.

ARTICLE II: PRIVACY AND SECURITY OF PERSONAL INFORMATION

1. **Compliance with Law.**
When providing services pursuant to this Contract, Contractor may have Access to or receive disclosed Personal Information that is regulated by one or more New York and federal laws and regulations, among them, but not limited to, the Family Educational Rights and Privacy Act at 12 U.S.C. § 1232g (34 CFR Part 99); Children's Online Privacy Protection Act at 15 U.S.C. §§ 6501-6502 (16 CFR Part 312); Protection of Pupil Rights Amendment at 20 U.S.C. § 1232h (34 CFR Part 98); the Individuals with Disabilities Education Act at 20 U.S.C. § 1400 et seq. (34 CFR Part 300); the New York Education Law at § 2-d (8 NYCRR Part 121); the New York General Business Law at article 39-F, and the New York Personal Privacy Protection Law at Public Officers Law article 6-A. Contractor agrees to maintain the confidentiality and security of Personal Information in accordance

with (a) applicable New York, federal and local laws, rules and regulations, and (b) NYSED's Data Privacy and Security Policy. Contractor further agrees that neither the services provided nor the manner in which such Services are provided shall violate New York, federal and/or local laws, rules and regulations, or NYSED's Data Privacy and Security Policy.

2. **Authorized Use.**
Contractor agrees and understands that it has no property, licensing or ownership rights or claims to Personal Information Accessed by or Disclosed to Contractor for the purpose of providing services, and Contractor must not use Personal Information for any purpose other than to provide the Services. Contractor will ensure that its Subcontractors agree and understand that neither the Subcontractor nor Contractor has any property, licensing or ownership rights or claims to Personal Information Accessed by or Disclosed to Subcontractor for the purpose of assisting Contractor in providing Services.

3. **Contractor's Data Privacy and Security Plan**.
Contractor shall adopt and maintain administrative, technical, and physical safeguards, measures, and controls to manage privacy and security risks and protect Personal Information in a manner that complies with New York State, federal and local laws, rules, and regulations and NYSED policies. Contractor shall provide NYSED with a Data Privacy and Security Plan that outlines such safeguards, measures, and controls to comply with (a) the terms of this DPA, (b) all applicable state, federal and local data privacy and security requirements and (c) NYSED's Data Privacy and Security Policy. Contractor's Data Privacy and Security Plan is attached as DPA Exhibit 1.

4. **Right of Review and Audit.**
Upon NYSED's request, Contractor shall provide NYSED with copies of its policies and related procedures that pertain to the protection of Personal Information. In addition, Contractor may be required to undergo an audit of its privacy and security safeguards, measures and controls as it pertains to alignment with the requirements of New York State laws and regulations performed by an independent third party at Contractor's expense, and provide the audit report to NYSED. In lieu of performing an audit, Contractor may provide NYSED with an industry standard independent audit report on Contractor's privacy and security practices that was issued no more than twelve months before the date NYSED informed contractor that it was required to undergo an audit.

5. **Contractor's Employees and Subcontractors**.
   (a) Contractor shall only provide Access or Disclose Personal Information to Contractor's employees and Subcontractors who need to know the Personal Information to provide the Services and the Access to or Disclosure of Personal Information shall be limited to the extent necessary to provide such Services. Contractor shall ensure that all such employees and Subcontractors comply with the terms of this DPA.

(b) Contractor must ensure that each Subcontractor is contractually bound by a written agreement that includes confidentiality and data security obligations equivalent to, consistent with, and no less protective than, those found in this DPA.

(c) Contractor shall examine the data privacy and security measures of its Subcontractors. If at any point a Subcontractor fails to materially comply with the requirements of this DPA, Contractor shall: notify NYSED and remove such Subcontractor's Access to Personal Information; and, as applicable, retrieve all Personal Information received or stored by such Subcontractor and/or ensure that Personal Information has been securely deleted and destroyed in accordance with this DPA. In the event there is an incident in which Personal Information is unlawfully Accessed or Disclosed or compromised by Subcontractor, Contractor shall follow the Data Breach reporting requirements set forth in Section 9 of this DPA.

(d) Contractor shall take full responsibility for the acts and omissions of its employees and Subcontractors.

(e) Other than Contractor's employees and Subcontractors who have a need to know the information, Contractor must not provide Access to or Disclose Personal Information to any other party unless such Disclosure is required by statute, court order or subpoena, and the Contractor notifies NYSED of the court order or subpoena no later than the time the information is Disclosed, in advance of compliance but in any case, provides notice to NYSED no later than the time the Personal Information is Disclosed, unless such disclosure to NYSED is expressly prohibited by the statute, court order or subpoena. Notification shall be made in accordance with the Notice provisions of this Contract and shall also be provided to the Office of the Chief Privacy Officer, NYS Education Department, 89 Washington Avenue, Albany, New York 12234.

(f) Contractor shall ensure that its Subcontractors know that they cannot provide Access to or Disclose Personal Information to any other party unless such Access or Disclosure is required by statute, court order or subpoena. If a Subcontractor is required to provide Access to or Disclose Personal Information pursuant to a court order or subpoena, the Subcontractor shall, unless prohibited by statute, court order or subpoena, notify Contractor no later than two (2) days before any Personal Information is Accessed or Disclosed. Upon receipt of notice from a Subcontractor, Contractor shall provide notice to NYSED no later than the time that the Subcontractor is scheduled to provide Access or Disclose the Information.

6. Training.

Contactor shall ensure that all its employees and Subcontractors who have Access to Personal Information have received or will receive training on the federal and state laws governing confidentiality of such Personal Information prior to receiving Access.

7. **Data Return and Destruction of Data**.

(a) Contractor is prohibited from retaining Disclosed Personal Information or continuing to Access Personal Information , including any copy, summary or extract of Personal Information, on any storage medium (including, without limitation, secure data centers and/or cloud-based facilities, and hard copies) beyond the term of this Contract unless such retention is either expressly authorized by this Contract, expressly requested in writing by NYSED for purposes of facilitating the transfer of Personal Information to NYSED, or expressly required by law. As applicable, upon expiration or termination of this Contract, Contractor shall transfer the Disclosed Personal Information to NYSED, in a format and manner agreed to by the Parties.

(b) When the purpose that necessitated Contractor's Access to and/or Disclosure of Personal Information has been completed or Contractor's authority to have Access to Personal Information or retain Disclosed information has expired, Contractor shall ensure that all Personal Information (including without limitation, all hard copies, archived copies, electronic versions, electronic imaging of hard copies) as well as any and all Personal Information maintained on behalf of Contractor in a secure data center and/or cloud-based facilities that remain in the possession of Contractor or its Subcontractors is securely deleted and/or destroyed in a manner that does not allow it to be retrieved or retrievable, read or reconstructed. Hard copy media must be shredded or destroyed such that Personal Information cannot be read, or otherwise reconstructed, and electronic media must be cleared, purged, or destroyed such that the Personal Information cannot be retrieved. Only the destruction of paper Personal Information, and not redaction, will satisfy the requirements for data destruction. Redaction is specifically excluded as a means of data destruction.

(c) Contractor shall provide NYSED with a written certification of the secure deletion and/or destruction of Personal Information held by the Contractor or Subcontractors to this Contract at the address for notifications set forth in this Contract.

(d) To the extent that Contractor and/or its Subcontractors continue to be in possession of any de-identified Personal Information (i.e., Personal Information that has had all direct and indirect identifiers removed), Contractor agrees that neither it nor its Subcontractors will attempt to re-identify de-identified Personal Information and/or transfer de-identified Personal Information data to any person or entity, except as provided in subsection (a) of this section.

8. **Encryption.**

Contractor shall use industry standard security measures including encryption protocols that comply with New York law and regulations to preserve and protect Personal Information. Contractor must encrypt information at rest and in transit in accordance with applicable New York laws and regulations.

9. **Commercial or Marketing Use Prohibition.**
Contractor agrees that it will not sell, use, or Disclose Personal Information for a Commercial or Marketing Purpose and that it will contractually prohibit its Subcontractors from the same.

10. **Breach**.
Contractor shall promptly notify NYSED of any Breach of Personal Information, regardless of whether Contractor or Subcontractor suffered the Breach, without delay and in the most expedient way possible, but in no circumstance later than seven (7) calendar days after discovery of the Breach. Notifications shall be made in accordance with the notice provisions of this Contract and shall also be provide to the Office of the Chief Privacy Officer, NYS Education Department, 89 Washington Avenue, Albany, New York 12234 and must include a description of the Breach which includes the date of the incident and the date of discovery; the types of Personal Information affected, and the number of records affected; a description of Contractor's investigation; and the name of a point of contact.

11. **Cooperation with Investigations.**
Contractor and its Subcontractors will cooperate with NYSED, and law enforcement where necessary, in any investigations into a Breach. Any costs incidental to the required cooperation or participation of the Contractor will be the sole responsibility of the Contractor if such Breach is attributable to Contractor or its Subcontractors.

12. **Notification to Individuals.**
Where a Breach of Personal Information occurs that is attributable to Contractor and/or its Subcontractors, Contractor shall pay for or promptly reimburse NYSED the full cost of NYSED's notification to the affected individuals, where applicable. NYSED will be reimbursed by Contractor within 30 days of a demand for payment under this section.

13. **Termination**.
The confidentiality and data security obligations of Contractor under this DPA shall continue for as long as Contractor or its Subcontractors retain Disclosed Personal Information or Access to Personal Information and shall survive any termination of the Agreement to which this DPA is attached.

DPA EXHIBIT 1 - Contractor's Data Privacy and Security Plan

NYSED has adopted the NIST Cybersecurity Framework as its' standard to protect Personal Information. For contracts where a Contractor may have access to Personal Information, the Contractor must complete the following or provide a plan that materially addresses its requirements, including alignment with the NIST Cybersecurity Framework, which is the standard for educational agency data privacy and security policies in New York state**. While this plan is not required to be posted to NYSED's website, contractors should nevertheless ensure that they do not include information that could compromise the security of their data and data systems.**

1. Outline how you will implement applicable data privacy and security contract requirements over the life of the Contract

2. Specify the administrative, operational, and technical safeguards and practices that you have in place to protect Personal Information.

3. Address the training received by your employees and any Subcontractors engaged in the provision of services under this Contract on the federal and state laws that govern the confidentiality of Personal Information.

4. Outline contracting processes that ensure that your employees and any Subcontractors are bound by written agreement to the requirements of this Contract, at a minimum.

5. Specify how you will manage any data privacy and security incidents that implicate Personal Information and describe any specific plans you have in place to identify breaches and/or unauthorized disclosures, and to meet your obligations to report incidents to NYSED.

6. Describe how data will be transitioned to NYSED when no longer needed by you to meet your contractual obligations, if applicable.

7. Describe your secure destruction practices and how certification will be provided to NYSED.

8. Outline how your data privacy and security program/practices align with NYSED's Data Privacy and Security Policy.

Production Blackout Schedule

Month	Dates
January	Week before and including the 15th
January	Week before and including the 31st
Feburary	First business day
Feburary	15th through the 29th
March	Week before and including the 15th
March	Week before and including the 31st
April	Week before and including the 30th
May	Week before and including the 31th
June	Week before and including the 15th
June	Week before and including the 30th
July	Week before and including the 31th
August	Week before and including the 15th
September	First business day
September	Week before and including the 15th
September	Week before and including the 31st
October	Week before and including the 15th
November	Week before and including the 15th
December	Week before and including the 15th

	NEW YORK STATE EDUCATION DEPARTMENT Performance Improvement & Management Services (PIMS) Information Security Office (ISO) 89 Washington Avenue, Room 280 EBA Albany, NY 12234 Telephone: (518) 473-5469 Fax: (518) 474-2519 Email: infosec@nysed.gov	**NYSED ISO POLICY** Acceptable Use of Information Technology (IT) Resources No:SECP3 - V:1.0 - Updated: 12/29/2016
Issued By: NYSED Chief Information Security Officer		**Owner:** NYSED Information Security Office

1.0 Purpose and Benefits of the Policy

The Information Security Office Mission is to safeguard the confidentiality, integrity, and availability of Department information. The Information Security Office develops information security policies, standards, and guidelines for the Department.

The purpose of this policy is to define and to establish the acceptable use of Department Information Technology (IT) resources.

Acceptable organizational use of IT resources and effective security require the participation and support of the Department workforce ("users"). Unacceptable use exposes the Department to potential risks including malware attacks, compromise of network systems and services, and legal liability.

The benefit to the Department will be an enhanced security of Departmental Information through proper use of all Department IT resources.

2.0 Scope

This policy applies to all Department IT resources and all users of such resources.

It is the responsibility of users to read and understand this policy and to conduct their activities in accordance with its terms. In addition, users must read and understand the NYSED Information Security Policy and its associated standards.

3.0 Information Statement

Except for any privilege or confidentiality recognized by law, individuals have no legitimate expectation of privacy during any use of the Department's IT resources or in any data on those resources. Any use may be monitored, intercepted, recorded, read, copied, accessed or captured in any manner including in real time, and used or disclosed in any manner, by authorized personnel without additional prior notice to individuals. Periodic monitoring will be conducted of systems used, including but not limited to all computer files and all forms of electronic communication, including email, text messaging, instant messaging, telephones, computer systems and other electronic records. In addition to the notice provided in this policy, warning banner text at system entry points where users initially sign on may notify users about this monitoring and remind users that unauthorized use of the Department's IT resources is not permissible.

At the discretion of its executive management, the Department may impose restrictions on the use of a particular information technology resource. For example, the Department may block access to certain websites or services not serving legitimate business purposes or may restrict a user's ability to attach devices to the Department's information technology resources (e.g., personal USB drives, iPods).

Acceptable Use

All uses of information technology resources must comply with Department policies, standards, procedures, and guidelines, as well as any applicable Federal, State and local laws, including copyright laws and licensing agreements.

Consistent with the foregoing, acceptable use of information technology resources encompasses the following duties:

- Protection of confidential information from unauthorized use or disclosure;
- Observing authorized levels of access and utilizing only approved information technology devices or services; and
- Immediately reporting suspected computer security incidents to the appropriate manager and the Information Security Office (ISO).

Unacceptable Use

The following list is not intended to be exhaustive, but is an attempt to provide a framework for activities that constitute unacceptable use of Department IT resources. Users may be exempted from one or more of these restrictions (e.g., storage of objectionable material in the context of a disciplinary matter), during the course of their authorized job responsibilities, after approval from Department executive management, in consultation with the Department IT staff.

Unacceptable use includes the following:

- Distributing, transmitting, posting, or storing any electronic communications, material or correspondence that is threatening, obscene, harassing, pornographic, offensive, defamatory, discriminatory, inflammatory, illegal, or intentionally false or inaccurate;

- Purporting to represent the Department in matters unrelated to official authorized job duties or responsibilities;

- Connecting unapproved devices to the Department network or any Department information technology resource;

- Connecting Department information technology resources to unauthorized networks;

- Connecting to any wireless network while physically connected to a Department wired network;

- Installing, downloading, or running software that has not been approved following appropriate security, legal, and/or IT review in accordance with Department policies;

- Connecting to commercial email systems (e.g., Gmail, Hotmail, Yahoo) without prior management approval (the Department recognizes the inherent risk in using commercial email services as email is often used to distribute malware);

- Using Department information technology resources to circulate unauthorized solicitations or advertisements for non-Department purposes including religious, political, or not-for-profit entities;

- Providing unauthorized third parties, including family and friends, access to the Department IT resources or facilities;

- Using Department information technology resources for commercial or personal purposes, in support of religious, political, not-for-profit business, or for-profit business activities or in support of other outside employment or business activity (e.g., consulting for pay, business transactions);

- Propagating chain letters, fraudulent mass mailings, spam, or other types of undesirable and unwanted email content using Department information technology resources; and

- Tampering, disengaging or otherwise circumventing Department or third-party IT security controls.

Occasional and Incidental Personal Use

Occasional and incidental personal use of information technology resources is permitted, provided such use is otherwise consistent with this policy, is limited in amount and duration, and does not impede the ability of the individual or other users to fulfill the Department's responsibilities and duties, including but not limited to, extensive bandwidth, resource, or storage utilization. The Department may revoke or limit this privilege at any time.

If you are unclear about the acceptable "personal" use of a Department-provided resource, seek authorization from your immediate supervisor.

Individual Accountability

Individual accountability is required when accessing all IT resources. Each individual is responsible for protecting against unauthorized activities performed under their user ID. This includes locking your computer screen when you walk away from your system and protecting your credentials (e.g., passwords, tokens or similar technology) from unauthorized disclosure, including sharing. Credentials must be treated as confidential information, and must not be disclosed or shared.

Restrictions on Off-Site Transmission and Storage of Information

Users must not transmit non-public, confidential, sensitive, or restricted Department information to or from personal email accounts (e.g., Gmail, Hotmail, Yahoo) or use a personal email account to conduct Department business unless explicitly authorized. Users must not store non-public, confidential, sensitive or restricted Department information on a non-Department issued device, or with a third-party file storage service that has not been approved for such storage by the Department. Users should be aware that their email account may be subject to Freedom of Information Law (FOIL) requests.

User Responsibility for Information Technology Equipment

Users are routinely assigned or given access to information technology equipment in connection with their official duties. This equipment belongs to the Department and must be immediately returned upon request or at the time an employee is separated from Department service. Users may be financially responsible for the value of equipment assigned to their care if it is not returned to the Department. Should Department IT equipment be lost, stolen or destroyed, users are required to provide a written report of the circumstances surrounding the incident. Users may be subject to disciplinary action which may include repayment of the replacement value of the equipment. The Department has the discretion to not issue or re-issue information technology devices and equipment to users who repeatedly lose or damage Department IT equipment.

Devices that contain Department information must be attended to at all times or physically secured and must not be checked in transportation carrier luggage systems.

Use of Social Media

The use of public social media sites to promote Department activities requires written pre-approval of the Department External Affairs Office (EAO). Approval is at the discretion of the EAO and may be granted upon demonstration of a business need and review and approval of service agreement terms by the Department Counsel's Office, if appropriate. Final approval by the EAO will define the scope of the approved activity, including, but not limited to, identifying approved users.

Unless specifically authorized by the Department, the use of Department email addresses on public social media sites is prohibited. In those instances in which users access social media sites on their own time utilizing personal resources, they must remain sensitive to expectations that they will conduct themselves in a responsible, professional, and secure manner with regard to references to the Department and Department staff. These expectations are outlined below.

a. Use of Social Media within the Scope of Official Duties

The Department EAO, or designee, must review and approve the content of any posting of public information, such as blog comments, tweets, video files, or streams, to social media sites on behalf of the Department. However, EAO approval is not required for postings to public forums for technical support, if participation in such forums is within the scope of the user's official duties, has been previously approved by his or her supervisor, and does not include the posting of any sensitive information, including specifics of the Department's information technology infrastructure. In addition, EAO approval is not required for postings to private Department approved social media collaboration sites (e.g., Yammer). Blanket approvals may be granted, as appropriate.

Accounts used to manage the Department's social media presence are privileged accounts and must be treated as such. These accounts are for official use only and must not be used for personal use. Passwords of privileged accounts must follow Department information security standards, be unique on each site, and must not be the same as passwords used to access other Department information technology resources.

Information posted online on behalf of the Department may be subject to the record retention/disposition provisions of the Arts and Cultural Affairs Law and may be subject to Freedom of Information Law (FOIL) requests.

b. Guidelines for Personal Use of Social Media

Staff should be sensitive to the fact that information posted on social media sites clearly reflects on the individual and may also reflect on the individual's professional life. Consequently, staff should use discretion when posting information on these sites and be conscious of the potential perceptions of and responses to the

information. It is important to remember that once information is posted on a social media site, it can be captured and used in ways not originally intended. It is nearly impossible to retract, as it often lives on in copies, archives, backups, and memory cache.

Users should respect the privacy of Department staff and not post any identifying information of any Department staff without permission (including, but not limited to, names, addresses, photos, videos, email addresses, and phone numbers). When you choose to post comments on social media sites, you are legally responsible for those comments.

If a personal email, posting, or other electronic message could be construed to be an official communication, a disclaimer is strongly recommended. A disclaimer might be: "The views and opinions expressed are those of the author and do not necessarily reflect those of the New York State Education Department or the State of New York."

Users should not use their personal social media accounts for Department official business, unless specifically authorized by the Department. Users are strongly discouraged from using the same passwords in their personal use of social media sites as those used for work, in order to prevent unauthorized access to Department resources in the event that the password is compromised.

4.0 Compliance

This policy shall take effect upon publication.

Any violation of this policy may subject the user to disciplinary action, civil penalties, and/or criminal prosecution. The Department will review alleged violations of this policy on a case-by-case basis and pursue recourse, as appropriate.

5.0 Definitions of Key Terms

Information Technology Resources – Equipment or services used to input, store, process, transmit, and output information, including, but not limited to, desktops, laptops, mobile devices, servers, telephones, fax machines, copiers, printers, Internet, email, and social media sites.

6.0 ISO Contact Information

Submit all inquiries and requests for future enhancements to the policy owner at:

NEW YORK STATE EDUCATION DEPARTMENT
Information Security Office
89 Washington Avenue, Room 280 EBA
Albany, NY 12234
Telephone (518) 473-5469
Fax (518) 474-2519
Email: infosec@nysed.gov

7.0 Review Schedule and Revision History

This policy shall take effect upon publication. The Information Security Office (ISO) shall review the policy at least once every year to ensure relevancy. To accomplish this assessment, ISO may issue, from time to time, requests for information to other office departments, which will be used to develop any reporting requirements as may be requested by the Department Chief Information Officer, the Board of Regents, or Legislative entities.

Date	Description of Change	Reviewer
3/10/2016	Original Policy Release	IT Governance Board Approval
12/29/2016	Updated policy header	Information Security Office
12/29/2017	Scheduled Policy Review	

8.0 Related Documents

- NYSED Information Security Policy

NEW YORK STATE EDUCATION DEPARTMENT Performance Improvement & Management Services (PIMS) Information Security Office (ISO) 89 Washington Avenue, Room 280 EBA Albany, NY 12234 Telephone: (518) 473-5469 Fax: (518) 474-2519 Email: infosec@nysed.gov	**NYSED STANDARD** Cybersecurity Incident Response (CIR) No:SECS1 - V:1.0 - Updated: 12/29/2016
Issued By: Information Security Office	**Owner:** Information Security Office

1.0 Purpose and Benefits of the Standard

The purpose of this standard is to establish the Department Cybersecurity Incident Response (CIR) method and general steps for responding to cybersecurity incidents. In addition to providing a standardized process flow, this standard:

(1) Identifies the Department Incident Response (IR) stakeholders and establishes their roles and responsibilities.

(2) Describes incident triggering sources, incident types, and incident severity levels.

(3) Includes requirements for annual testing, post-incident lessons-learned activities, and collection of IR metrics for use in gauging IR effectiveness.

The goals of IR, as outlined in this standard, are to:

- Confirm whether a cybersecurity incident occurred.
- Provide a defined incident notification process.
- Promote the accumulation and documentation of accurate information.
- Establish controls for proper retrieval and handling of evidence.
- Contain the incident and stop any unwanted activity quickly and efficiently.
- Minimize disruption to Department operations.
- Provide accurate reports and useful recommendations to management.
- Prevent and/or mitigate future incidents from occurring.

The benefit to the Department will be confidential, consistent, accurate, secure, effective, expedient, and efficient handling of all cybersecurity related incidents which affect the Department's wellbeing.

2.0 NYSED Information Security Office Mission

The Information Security Office Mission is to safeguard the confidentiality, integrity, and availability of Department information.

3.0 Scope

The scope includes response to all cybersecurity related incidents at the Department.

4.0 Information Statement

4.1 IR Stakeholder Roles and Responsibilities

In order to respond effectively to a cybersecurity incident, it is critical that all IR stakeholders fully understand not only their roles and responsibilities in the IR process, but also the roles and responsibilities of each IR stakeholder. This is necessary to:

(1) Avoid duplication of effort.

(2) Minimize procedural gaps that may occur.

(3) Ensure rapid response to cybersecurity incidents.

(4) Ensure that cybersecurity incidents are brought to the attention of the proper stakeholders, as warranted.

Department IR stakeholders include:

1. **Department Leadership** – holistically examines cybersecurity incidents, determines the overall risk to the Department, and decides on next steps, including if and when to report the incident to entities external to the Department. At minimum, this team includes the following staff (either appointed or acting):

    a. Executive Management
    b. Counsel
    c. Communications Chief
    d. Chief Privacy Officer (CPO)
    e. Chief Information Security Officer (CISO)
    f. Human Resources Director

2. **Department Cybersecurity Incident Response Team (CIRT)**– The Department's Chief Information Security Officer (CISO) will lead the CIRT. The CIRT will be a team of staff that serves as first responders to all cybersecurity incidents. The CIRT will handle incidents in a manner consistent with the Information Security Office Mission. The CIRT will utilize other ITS and Department staff as needed to produce the best incident response and outcome for the Department. At minimum, this team includes the following staff (either appointed or acting):

    a. Chief Information Security Officer (CISO)
    b. Core CIRT team staff – appointed by the CISO, Department IT staff members who are experts in their respective disciplines (e.g. Server, Database, and Applications Administrators) will complete the team.
    c. For incidents that require additional staff (including potential data breach incidents):
        i. Chief Privacy Officer (CPO)
        ii. Chief of Security
        iii. Information Owner – the program area executive that is ultimately responsible for their program area's data

iv. Information Steward – appointed by the Information Owner, serves as the subject matter (data) expert for the program area and ensures that all Department policies and procedures are followed in relation to the data
v. Additional First Responders - Department IT staff, such as network managers, system administrators, and other technical personnel, will be called upon, as needed, to provide support and tactical response to the CIRT team. All digital forensic analysis must be performed by, or under the direction of, the CIRT.

3. **State Chief Information Security Officer (State CISO)** – The State CISO, or his/her designee, provides for overall coordination of IR including the requisite extent of notifications for an incident. The State CISO leads the Enterprise Information Security Office (EISO) within the Office of Information Technology Services (OITS) which provides incident response services for NY State.

4. **EISO Cyber Incident Response Team (EISO CIRT)** – The EISO CIRT responds to incidents by providing hands-on technical IR. The EISO CIRT will also recommend steps for Department staff to remediate and mitigate such that it reduces the likelihood of future incidents.

5. **EISO Cyber Security Operations Center (CSOC)** – The EISO CSOC serves as a central group for collaboration and information sharing with other entities that may be experiencing the same or similar incidents, to help resolve the problem more quickly than if done separately. The EISO CSOC collects statewide information on the types of vulnerabilities that are being exploited and the frequency of attacks and shares preventative information to help other NY State Entities (SEs) protect themselves from similar attacks.

6. **External Entities** - In consultation with the EISO CIRT, external entities may conduct hands-on IR activities, such as investigative response activities, or may provide guidance. For example, a security solutions vendor may provide assistance on security appliance settings. External entities include vendors, service providers, educational entities, law enforcement including, but not limited to:

- New York State Intelligence Center (NYSIC)
- Multi-State Information Sharing and Analysis Center (MS-ISAC)
- New York State Police
- Federal Bureau of Investigation (FBI)
- Internet Service Providers
- Security Solutions Vendors
- Data Holder Vendors
- District Superintendents

4.2 IR Process Flow

This IR process flow covers how to respond to specific situations for IR stakeholders to ensure an effective and efficient response. The focus of the IR process is to eradicate the problem as quickly as possible, while gathering actionable intelligence, to restore business functions, improve detection and prevent reoccurrence. The Department has adopted a six step IR process flow as depicted below[1]:

[1]Based on the SANS Institute Incident Handling Step-by-Step

Figure 4.1 - Incident Response Process Flow

Step 1: Preparation

Proper planning and preparation for an incident before it occurs ensures a more effective and efficient IR process. Activities associated with this step, include establishing IR teams; updating IR tools, policies/procedures, and forms/checklists; and ensuring IR communication procedures and IR stakeholder contact lists are accurate and up-to-date. The Department must have a defined and up to date IR Stakeholder Contact List, and establish multiple communication channels with all entities and individuals on the IR Stakeholder Contact List.

As per NYS and NYSED Information Security Policy, all employees are required to report suspected cybersecurity incidents or weaknesses to the appropriate manager and to the Information Security Office (as further described in Section 5 of this document, 'Communication').

The CIRT will establish standard operating procedures (SOPs) for IR to reflect industry standards and best practice. These SOPs will be followed during incident response. Any exception must be documented. The CIRT must routinely vet and validate the tools and techniques used for IR. In order to operate efficiently and effectively, the IR process must be regularly tested. This must occur at least annually. This testing can be accomplished with mock incident training or tabletop exercises using realistic scenarios to provide a high-level outline and systematic walkthrough of the IR process and, to the extent possible, must include all IR stakeholders. These training scenarios must include specific 'discussion points' that represent key learning opportunities, and incorporate lessons-learned, which can then be integrated into the IR process as part of its review.

Step 2: Identification

Identification involves review of anomalies to determine whether or not an incident has occurred, and, if one has occurred, determining the nature of the incident. Identification begins with an event, an anomaly that has been reported or noticed in a system or network. Detection can be accomplished through technical sources (e.g. operations staff, anti-virus software), non-technical sources (e.g. user security awareness and reporting), or both.

It is important to recognize that not every network or system event will be a security incident. A first responder must be assigned to determine if there is an incident, categorize the incident and escalate as necessary. Typically, this will be the Information Security Office.

To be effective in IR, incidents must be classified, and brought to the attention of the proper IR stakeholders as soon as possible in order to promote collaboration and information sharing. Incident classification requires

the use of established incident categories together with an incident severity matrix as a means for prioritizing incidents and determining appropriate IR activities.

Incident Categories

It is important to categorize common incidents experienced throughout the enterprise. By doing so, IR stakeholders can better focus their IR activities. It should be noted that incidents can have more than one category and categorization may change as the investigation unfolds. The Department has adopted the six (6) US-CERT[2] incident categories as follows:

Incident Categories

Category	Name	Description
0	Exercise / Network Defense Testing	Used during state, federal, international exercises and approved activity testing of internal/external network defenses or responses.
1	Unauthorized Access	An individual gains logical or physical access without permission to a Department network, system, application, data, or other resource.
2	Denial of Service	An attack that successfully prevents or impairs the normal authorized functionality of networks, systems, or applications by exhausting resources. This activity includes being the victim of or participating in the Denial of Service (DoS).
3	Malicious Code	Successful installation of malicious software (e.g., virus, worm, Trojan horse, or other code-based malicious entity) that infects an operating system or application.
4	Improper Usage	A person who knowingly or unknowingly violates acceptable computing use policies.
5	Scans / Probes / Attempted Access	Includes any activity that seeks to access or identify a Department computer, open ports, protocols, service, or any combination to later exploit. This activity does not directly result in a compromise or denial of service. Unauthorized internal scans are considered incidents. Most external scans are considered to be routine, and on a case-by-case basis may require response and investigation.
6	Investigation	Unconfirmed incidents that are a potentially malicious or anomalous activity deemed by the reporting entity to warrant further review.

Table 4.2 – Incident Categories

Incident Severity Matrix

All information security incidents should be categorized according to severity level to assist in determining the extent to which a formal IR is required. Severity levels are based on the perceived business impact of the incident. Severity levels may change as the investigation unfolds. General definitions and description of each severity level are as follows:

[2] http://www.us-cert.gov/government-users/reporting-requirements

Incident Severity Matrix		
Level	**Definition**	**Examples**
High	Incidents that have a severe impact on operations	— Compromise of sensitive data — Widespread malcode attack — Unauthorized access to critical systems — DoS affecting the entire enterprise
Medium	Incidents that have a significant impact, or the potential to have a severe impact, on operations	— Small-scale DoS attack — Website compromises — Unauthorized access (brute force attacks against FTP, ssh, and other protocols)
Low	Incidents that have a minimal impact with the potential for significant or severe impact on operations	— Network probes or system scans — Isolated virus infections — Acceptable use violations

Table 4.3 – Incident Severity Matrix

Escalation Procedures

During an incident, clear and effective communication is critical. As such, an escalation procedure should address all lines of communication in the event an incident occurs. This includes not only internal communication but external communications as well. Communication should flow through all involved IR stakeholders so that everyone has the necessary information to act and carry out their responsibilities in a timely manner. Notification must be made as soon as possible but should not delay the Department from taking appropriate actions to isolate and contain damage.

The Department must have an IR escalation procedure that consists of:

(1) An escalation matrix
(2) An up-to-date contact list with alternate contacts
(3) Multiple communication channels

All in an effort to ensure appropriate and accurate information is disseminated quickly to the appropriate IR stakeholders (as further described in Section 5 of this document, 'Communication').

Incident Scoping

Initial scoping is provided by the Department and includes:

- Identifying potential targets (e.g., known compromised systems, likely affected systems, key systems);
- Defining external touch points (e.g., Internet, wireless, 3rd party, remote access connections);
- Prioritizing likely scenarios (e.g., internal vs. external threat, targeted attack vs. target of opportunity); and
- Visualizing in-scope environment (e.g., network diagram, data flow).

Considerations for incident scoping activities are as follows:

- Relying on relevant and verified evidence sources
- Reducing false positives and volume of data
- Avoiding excessive scope and 'scope creep'
- Realizing operational and resource limitations may affect scope

As additional incident-related information develops during the IR process and as additional stakeholders become involved, an incident typically requires re-scoping.

Incident Tracking & Reporting

A secure centralized tracking system, that can accommodate 'need to know' access, leads to a more efficient and systematic IR effort, as well as provides an audit trail should the efforts lead to legal prosecution of the threat.

At a minimum, documentation of the incident must contain the following information:

- Date / time the incident was reported
- Type of incident
- Reporting source of incident
- Summary of the incident
- Current status of the incident
- All actions taken concerning the incident
- Contact information for all involved parties
- Evidence gathered during incident investigation
- Relevant comments from IR team members
- Proposed next steps to be taken

Step 3: Containment

This step focuses on containing the threat to minimize damage. It is during this step that information is collected to determine how the attack took place. All affected systems within the enterprise should be identified so that containment (and eradication and recovery) is effective and complete.

Incident containment involves 'stopping the bleeding' and preventing the incident from spreading. Containment can be accomplished by isolating infected systems, blocking suspicious network activity, and disabling services, among other actions. Containment varies for each incident depending on the severity and risk of continuing operations. Department leadership makes decisions regarding containment measures based on recommendations from the EISO.

Step 4: Eradication

Eradication involves removing elements of the threat from the enterprise network. Specific eradication measures depend on the type of incident, number of systems involved, and the types of operating systems and applications involved. Typical eradication measures include reimaging infected systems and enhanced monitoring of system activity.

Analysis of information collected is an iterative process and occurs/reoccurs during both the containment and eradication phases.

Step 5: Recovery

Once the root cause of an incident has been eradicated, the recovery phase can begin. The goals of this step are to:

(1) Remediate any vulnerabilities contributing to the incident (and thus prevent future incidents).

(2) Recover by restoring operations to normal. A phased approach is often used to return systems to normal operation, harden them to prevent similar future incidents and heighten monitoring for an appropriate period of time. Typical recovery activities include rebuilding systems from trusted images/gold standards, restoring systems from clean backups and replacing compromised files with clean versions.

Care must be taken to ensure that files restored from backup do not reintroduce malicious code or vulnerabilities from the incident and that the system is clean and secure before returning to production use. Once recovery has been completed, the CISO must validate/certify that the incident has been resolved.

Step 6: Lessons Learned

An IR process is only as good as the ability to execute it successfully. Lessons learned can be the results of actual IR activities or IR capability testing, and these results should be used to improve the IR process by identifying systemic weaknesses and deficiencies and taking steps to improve on these. It is important that this take place relatively soon after the incident is closed.

Lessons learned, or post mortem, discussions provide:

(1) A record of steps taken to respond to an attack.

(2) Investigative results into determining the root cause of the attack.

(3) Potential improvements to make, such as IR stakeholder training and certifications, process and procedural updates, and technical modifications. Knowledge gained can be used in an effort to prevent and/or mitigate future incidents in the form of proactive services. This may include testing the IR process, conducting vulnerability assessments, providing computer security training, reviewing security policies and procedures, and disseminating cyber security reminders.

Both incident reports and the results of these lesson-learned discussions will be placed into a database for future use and shared with all IR stakeholders for situational awareness and professional development.

4.3 Incident Response Metrics

IR metrics must be compiled for each incident and reported to the Information Security Office for enterprise situational awareness when possible and practical.

These metrics allow IR stakeholders to:

(1) Measure IR effectiveness (and reveal potential gaps) over time.

(2) Identify trends in terms of threat activities.

(3) Provide justification for additional resources, to include additional personnel, training, and tools.

IR Metrics		
Category	Measurement	Description
Incidents	# Total Incidents / Year	Total amount of incidents responded to per year
	# Incidents by Type / Year	Total number of incidents by category responded to per year
Time	# Personnel Hours / Incident	Total amount of labor spent resolving incident
	# Days / Incident	Total amount of days spent resolving incident
	# System Down-Time Hours / Incident	Total hours of system down-time until incident resolved
Cost	Estimated Monetary Cost / Incident	Total estimated monetary cost per incident, to include containment, eradication, and recovery, as well as collection & analysis activities (this may include labor costs, external entity assistance, tool procurements, travel, etc.)
Damage	# Systems Affected / Incident	Total number of systems affected per incident
	# Records Compromised / Incident	Total number of records compromised per incident
Forensics	# Total Forensics Leveraged Incidents / Year	Total number of incidents requiring forensics (collection & analysis) per year
	# System Images Analyzed / Incident	Total number of system images analyzed per incident
	# System Memory Dumps Examined / Incident	Total number of system physical memory dumps examined per incident

Table 4.4 – Incident Response Metrics

5.0 Communication

As per NYS and NYSED Information Security Policy, all employees are required to report suspected cybersecurity incidents or weaknesses to the appropriate manager and to the Information Security Office.

Employees may contact the Information Security Office in any effective way possible:

- In person: Room 363 EBA
- By phone: 518-486-2354
- Through email: infosec@nysed.gov

- Contacting the IT Help Desk: 518-474-4357, option 2
- Completing the directions on the Cybersecurity Incident Report form

When informed of a suspected cybersecurity incident, the Department CIRT will work quickly to gather the facts and determine if an incident has actually occurred. Depending upon the severity of the incident, the CIRT may then advance directly through the remaining steps in the IR process flow in order to quickly minimize any damage resulting from the incident.

If it is clear that the incident is a potential breach of Department information, the CIRT will gather the facts as soon as possible and present the facts to Department Leadership so that next steps can be determined.

CIRT Call Tree – Additional staff may be called to help the CIRT perform incident response on an ad-hoc basis. The CIRT will refer to the Department's 'CIRT Call Tree' and will work to keep this list of IT staff updated as staff changes occur and will also review the list for overall accuracy on an annual basis.

Core CIRT team members will communicate in person, by phone, by email (SECCIRT distribution list), and in meetings.

NYSED Cyber Security Alert Level – This will be a visual indicator communicated to all NYSED staff on the AtWork-Information Security-NYSED Cyber Alert Level webpage (http://atwork.nysed.gov/iso/alerts/) so that staff may quickly understand the current level of cyber security concern at NYSED. CIRT will decide when the level needs to be adjusted and the webpage will be updated accordingly.

6.0 Definitions of Key Terms

Cybersecurity Event: An anomaly that has been reported or noticed in a system or network.

Cybersecurity Incident: A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices. A computer security incident is also defined as any event that adversely affects the confidentiality, integrity, or availability of a system and its data.

Computer Network Defense (CND): Using defensive measures in order to protect information, information systems, and networks from threats.

Electronic Evidence: Electronic evidence as defined by the US DOJ Electronic Crime Scene Investigation is information and data of investigative value that is stored on or transmitted by an electronic device.

Incident Response: The manual and automated procedures used to respond to reported network intrusions (real or suspected); network failures and errors; and other undesirable events.

Incident Response Stakeholders: IR Stakeholders are any individuals – technical or non-technical, directly responding to or overseeing IR activities.

7.0 Contact Information

NEW YORK STATE EDUCATION DEPARTMENT
Information Security Office
89 Washington Avenue, Room 280 EBA

Albany, NY 12234
Telephone (518) 473-5469
Fax (518) 474-2519
Email infosec@nysed.gov

8.0 Review Schedule and Revision History

Date	Description of Change	Reviewer
3/10/2016	Original Release	IT Governance Board Approval
12/29/2016	Updated header, changed titles 'Data Owners/Stewards' to 'Information Owners/Stewards'	Information Security Office
12/29/2017	Scheduled Review	

9.0 Related Documents

- NYSED Information Security Policy http://atwork.nysed.gov/itm/policies/infosecpol.htm
- NYS OITS 'Cyber Incident Response' Standard No: NYS-S13-005 https://www.its.ny.gov/document/cyber-incident-response-standard
- NIST SP 800-61, Computer Security Incident Handling Guide
- NIST SP 800-83, Guide to Malware Incident Prevention and Handling
- NIST SP 800-86, Guide to Integrating Forensic Techniques into Incident Response
- New York State Cyber Incident Reporting Procedures

NEW YORK STATE EDUCATION DEPARTMENT Information Security Office (ISO) 89 Washington Avenue Albany, NY 12234	**NYSED ISO POLICY** Cybersecurity Incident Response Policy **No: SECP9 - V:13.0: (Rev 1/14/2020)**
Issued By: NYSED Chief Information Security Officer	**Owner:** NYSED Information Security Office

1. Purpose

   This policy outlines SED's plan to respond to incidents that threaten the confidentiality, integrity or accessibility of its data and data systems in a way that minimizes impact and disruption.

2. Scope

   This policy applies to incidents where the confidentiality, integrity or accessibility of the Department's data systems and data are threatened.

3. Procedure

   a. Employees must report suspected incidents that threaten the confidentiality, integrity or availability of the Department's data systems or data to the Information Security Office and their immediate supervisor or manager.
   b. If a critical incident is verified, the Chief Information Security Officer will convene a meeting of the Department's Incident Response Team (IR Team) and notify senior management.
   c. Where there has been a breach of Personally Identifiable Information (PII), the Chief Privacy Officer will be notified and will coordinate the process of compliance with notification requirements.
   d. Communication with the media, executive branch and Board of Regents must be coordinated with the Office of Communications.

4. Contact Information

   Information Security Office
   Email: infosec@nysed.gov
   Website: http://atwork.nysed.gov/iso/

   Chief Privacy Officer
   89 Washington Avenue, Albany, NY 12234

Telephone: (518) 474-0937
Email: privacy@its.ny.gov
Website: http://www.nysed.gov/data-privacy-security

NYS Education Department ITS Help Desk
Telephone: (518) 474-4357, option 2
Email: HELPDESK@nysed.gov

5. Review Schedule and Revision History

Date	Description of Change	Reviewer
7/31/2019	Draft	CPO, IRS
12/05/2019	Reviewed, Updated Contact Information, update user account definition	ITS, CPO, CISO, IRS
12/31/2019	Updated header, format, and contact information	CISO
1/14/2020	Updated 3c information; removed external resources paragraph	CISO
1/17/2020	Original Standard Release	CISO

NEW YORK STATE EDUCATION DEPARTMENT Information Security Office 89 Washington Avenue Albany, NY 12234	**NYSED ISO POLICY** Data Classification Policy **No: SECP7 - V:6.0 (8/11/2020)**
Issued By: NYSED Chief Information Security Officer	**Owner:** NYSED Information Security Office

1.0 Purpose and Benefits of the Policy

The policy establishes the data classification process for protecting the confidentiality, integrity, and availability of all data the New York State Education Department (SED) produces or is the custodian of both public and internal, written, and electronic.

This policy will adopt and apply the National Institute Standards and Technology Cybersecurity Framework (NIST CSF), regarding the New York State Education Department data classification process. Data classification is the basis for identifying an initial baseline set of security controls for data, data systems, and evaluation of retention and disposition schedules.

2.0 Scope

This policy applies to all data or information that is created, collected, stored, processed or managed by SED, or SED business partners, through its entire life cycle (i.e., generation, use, storage, and disposition); in electronic or non-electronic formats.

3.0 Requirements

All data created or used in support of SED business operations are owned by SED, regardless of form or format.

All data must be assigned a classification level, per the NYSED Information Security Policy.

The data classification level should be based upon the potential impact on SED; should certain events occur which interferes with the data or data systems needed to accomplish its assigned mission, responsibilities, and asset protection. Data classification must be reviewed on an ongoing basis to ensure that it has the appropriate classification level.

SED has established three data classification levels for the potential impact on the Department or individuals in the event of a data breach of security. The levels are defined as public information, restricted information, and confidential information. Each office should review the impact levels and apply them within the context of their operational environment.

The data classification levels to be used are as follows:

Public Information – Public Information is information accessible under the Freedom of Information Law and is available to any person, without regard for one’s status or interest.

Restricted Information – Restricted Information pertains to information, which is not public information, but can be disclosed to or used by SED representatives to carry out their duties, and anything that is not protected by regulation or law.

Examples of Restricted Information may include but are not limited to:

- Operational information
- Personnel records
- Information security procedures
- Research
- Internal communications

Confidential Information – Confidential Information is information that is prohibited from disclosure by law. Access to confidential information is limited to those SED representatives who need such information to carry out their duty. When confidential information is received from another office, the receiving office must accept the responsibility for the confidential information and secure it appropriately.

Examples of Confidential Information may include but are not limited to:

- Personally Identifiable Information (PII), such as name in combination with Social Security number (SSN) and/or financial account numbers
- Intellectual property, such as vendor or third-party copyrights, patents
- Passwords used for authenticating individuals
- Network architecture schematics

Table 1 shows the data classification impact level definitions used in NIST 800-60 Vol 2 based on data classification.

	Potential Impact[1]		
	LOW	**MODERATE**	**HIGH**
Confidentiality[2] A loss of confidentiality is the unauthorized disclosure of information. Consider the adverse effect on data types such as: • SED Mission/Programs • Personally Identifiable Information (PII) • System security plans • Organization Reputation	The unauthorized disclosure of information could be expected to have a **limited or no adverse effect** on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious adverse effect** on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic adverse effect** on organizational operations, organizational assets, or individuals.
Integrity A loss of integrity is the unauthorized modification or destruction of information. Consider the adverse effect on data types such as: • SED Mission/Programs	The unauthorized modification or destruction of information could be expected to have a **limited or no adverse effect** on	The unauthorized modification or destruction of information could be expected to have a **serious adverse effect** on	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic adverse effect** on

[1] NIST SP 800-60 Volume 2, Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories: http://csrc.nist.gov/publications/nistpubs/800-60-rev1/SP800-60_Vol2-Rev1.pdf

[2] FIPS Publication 199, Standards for Security Categorization of Federal Information and Information Systems: http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf

• Personally Identifiable Information (PII) • System security plans • Organization Reputation	organizational operations, organizational assets, or individuals.	organizational operations, organizational assets, or individuals.	organizational operations, organizational assets, or individuals.
Availability A loss of availability is the disruption of access to or use of information or an information system. Consider the adverse effect on data types such as: • SED Mission/Programs • Personally Identifiable Information (PII) • System security plans • Organization Reputation	The disruption of access to or use of information or an information system could be expected to have a **limited or no adverse effect** on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious adverse effect** on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic adverse effect** on organizational operations, organizational assets, or individuals.

(Table 1)

Guidelines for Classification

The guidelines listed below must be evaluated by SED departments when assigning classification to their data assets.

1. ***A written or electronic inventory of all SED data assets***.
    a. The inventory should be maintained and arranged by group or category. For a more efficient application of security controls a narrow grouping may be useful to assist with precise targeting of controls.
    b. An asset must be classified at the highest level necessary based upon the data elements (e.g., financial server, payroll spreadsheet).
    c. Any data that is reproduce, must also have the same classification as the original data set. If the confidentiality classification of data stored electronically cannot be determined than it must be classified as restricted information at a minimum.
    d. If multiple data assets have the potential to be merged together or resides in the same location (e.g., server), the classification must be of the higher classification.
2. ***Laws and Regulations***
    a. Ensure that all local, state, and federal laws, regulations, policies and standards relating to the data is adhered to.
    b. Account for ethical and privacy considerations.
    c. Any questions relating to the relevancy of any laws, regulations, policies and standards should be directed to the Office of Counsel.
3. ***Risk of loss of confidentiality, integrity, and availability***
    a. Information must be classified based upon its value, sensitivity, misused, consequences if lost, and any state or federal requirements.
4. ***Data Sharing and Contractual Agreements***
    a. If an agreement states that the recipient in the Department may share the data; the subsequent recipients must adhere to the requirements of the original classification unless the data has been modified and warrants a different classification.
5. ***All information assets must have an Information Owner.***
    a. The responsibility for the classification and control of an information asset must be at the manger or executive level who is ultimately responsible for the confidentiality, integrity and availability of that information.
    b. Information owners must assign a classification to data/assets they own or oversee. The classification should be done by group or category.

c. Information owners must determine access privileges and maintain access security controls for data custodians based upon the individual's duties.
d. Information custodians are individuals, groups, units, or departments responsible for implementing the security controls for the data assets based upon the classification level.

Data Classification Process

SED Business Offices are responsible for developing a data classification process within the scope of their responsibilities.

The classification of data must be determined by the potential impact (high, moderate, low) for each principle of security in the confidentiality, integrity, availability (CIA) model as reflected in Table 1. The business offices must develop a formal process for granting and revoking access to SED data. A risk assessment must be performed to inform and assist managers to determine the appropriate controls that will ensure the proper level of protection for the data.

Data owners should work with subject matter experts such as the Office of Counsel, the Privacy Office, or the Information Security Office in determining if existing laws, regulations or agreements; limit or regulate the collection, use or transfer of SED owned data.

Labeled information will assist SED personnel with the necessary guidance to provide a consistent and appropriate classification determination.

Data Encryption

All electronically stored or transmitted data classified as Confidential Information or Restricted Information shall be encrypted while it is either at rest or in transit, using an approved cryptographic algorithm. All media containing SED data assets must be stored and shared, in a manner consistent with its security classification.

All non-public Asymmetric cryptographic keys as well as the resources used to generate and store the cryptographic keys shall be considered Confidential Information.

As defined by the National Institute of Standards and Technology ISO/IEC 18033-3, the minimum recommended encryption key will be AES 128-bit or stronger.

Legal Review

SED program offices in partnership with the Office of Counsel shall coordinate a legal review of all SED data classification labels to ensure compliance with all local, state, and federal laws or regulations that regulate the use or access of the data asset.

4.0 Compliance

This policy shall take effect upon publication. The Information Security Office (ISO) shall review the policy at least once every year to ensure relevancy. To accomplish this assessment, the ISO may issue requests for information from other program office departments. The information garnered will be used to develop any reporting requirements as may be requested by the Department's Chief Privacy Officer, the Board of Regents, or Legislative entities.

Any violation of this policy may subject the user to disciplinary action up to and including termination. The Department will review alleged violations of this policy on a case-by-case basis and pursue recourse, as appropriate.

5.0 ISO Contact Information

Submit all inquiries and requests for future enhancements to the policy owner at:

NEW YORK STATE EDUCATION DEPARTMENT
Information Security Office
Website: http://atwork.nysed.gov/iso/
Email: infosec@nysed.gov

6.0 Review Schedule and Revision History

Date	Description of Change	Reviewer
7/24/2019	DRAFT	CISO
1/27/2020	Subcommittee Review	
4/21/2020	Information Security Committee Review	ISC
4/27/2020	Update compliance section, update classification levels, update data sharing agreement	CISO
5/19/2020	Section 1 Purpose and Benefits of the Policy: • The phrase “apply the Federal Information Processing Standards (FIPS), the National Institute Standards and Technology (NIST) Special publications”, has been removed as these standards do not apply to the data classification policy Section 2 Scope: • The sentence “This policy applies to all SED employees, whether permanent or non-permanent, full or part-time, contractors, consultants, vendors, and business partners, who have access to or manage SED data”, has been removed to simplify the scope and remove any potential ambiguity. Section 3 Requirements: • Examples for Restricted and Confidential Information has been added. • The Note: “Prior to the external release of any information please consult with the SED’s Data Privacy and Security Policy”, has been removed. • The title “Required Considerations for Classification” has been changed to “Guidelines for Classification” - Bullet 4. Title “Data Sharing Agreements and Contractual Requirements” has been changed to “Data Sharing and Contractual Agreements”, also removed the multiple contractual agreements types and highlighted “If an agreement states that the recipient in the Department may share the data; the subsequent recipients must adhere to the requirements of the original classification unless the data has been modified and warrants a different classification”	CISO

	Section 4 Compliance: • Updated the violation of the policy to be consistent with HR policies language	
8/11/2020	Update requirements language for consistency in regard to the term data classification	CISO
10/01/20	Original Standard Release	

7.0 Related Documents

- NYSED Data Privacy and Security Policy
- NYSED Information Security Policy
- NIST SP 800-60 Volume 2, Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories: http://csrc.nist.gov/publications/nistpubs/800-60-rev1/SP800-60_Vol2-Rev1.pdf
- FIPS Publication 199, Standards for Security Categorization of Federal Information and Information Systems: http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf
- New York State Information Classification Standard

NEW YORK STATE EDUCATION DEPARTMENT'S

DATA PRIVACY AND SECURITY POLICY

Table of Contents

1 INTRODUCTION

1.1 PURPOSE

The New York State Education Department (SED) has the responsibility for developing and implementing an effective data privacy and information security program. This policy document is a critical component of the program as it outlines the minimum requirements necessary to ensure the confidentiality, integrity, and availability of SED Information Technology (IT) assets and data. This includes all SED information systems and communication networks, whether owned, leased or rented by SED, and the information stored, processed, and transmitted on or by these systems and networks. This policy shall be published on SED's website.

1.2 OBJECTIVE

The objective of this policy is to address SED's responsibility to adopt appropriate administrative, technical and physical safeguards and controls to protect and maintain the confidentiality, integrity and availability of its IT assets and data. In addition, these policies ensure SED 's adherence to applicable legal and regulatory requirements and conform to best practices across the entire data and IT system lifecycle of creation, collection, retention, dissemination, protection, and destruction.

1.3 SCOPE

This policy document applies to all SED employees, interns, volunteers, consultants, and third parties who receive or have access to SED IT assets or data.

1.4 OVERSIGHT

SED's Chief Privacy Officer shall annually report to the Board of Regents on data privacy and security activities, the number and disposition of reported breaches, if any, and a summary of any complaints submitted pursuant to Education Law §2-d. While this policy falls under the program purview of the Chief Privacy Officer, it is the product of the collaborative efforts and expertise of the Chief Privacy Officer, Chief Information Officer and Chief Information Security Officer and their staff.

1.5 DOCUMENT STRUCTURE

This document is organized as follows:

- Section 1 is the introduction and introduces the policies, outlines the purpose, and establishes the implementation applicability.

- Section 2 defines the roles and responsibilities for individuals tasked to oversee and manage the SED data privacy and information security program.
- Sections 3-10 provide a comprehensive set of privacy and cybersecurity policy statements. The policy statements are organized by function and include privacy and governance, asset management, access control, awareness and training, data security, information protection, maintenance, and anomalies and events. The headings align to SED's chosen cybersecurity framework – the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) categories. Where applicable, NIST CSF categories were merged and additional requirements added to better align to the SED organization and mission.

2 ROLES AND RESPONSIBILITIES

SED has established and appointed applicable roles with the mission to coordinate, develop, implement, and maintain the data privacy and information security program. The roles listed below identify these positions and the specific activities personnel are responsible for executing. The Chief Privacy Officer, CIO and CISO must work with their respective governance boards and external partners to implement and maintain policies that protect the confidentiality, integrity and accessibility of SED IT systems and data.

- The Chief Privacy Officer (CPO) is responsible for establishing the protection framework for managing data privacy risk and the risk of the loss of confidentiality and integrity of SED data, and managing the collection, use and disclosure of personal information by establishing policies, procedures, and practices in accordance with applicable laws, rules, regulations, SED policies, and recommended industry practices. The Chief Privacy Officer will coordinate the implementation of a data governance strategy and lead SED's Data Privacy Governance Board as part of that framework. Data privacy and protection activities must be integrated into SED's management activities, including strategic planning, capital planning, and system design and architecture.
- The Chief Information Officer (CIO) is responsible for ensuring that information technology systems, programs, and the data they utilize, process and store are secure and protected from unauthorized access, alteration, damage, or release to or access by unauthorized persons.
- The Chief Information Security Officer (CISO) is responsible for establishing the information security governance framework and overseeing SED's implementation of information security. Information security activities must be integrated into other management activities of the enterprise, including strategic planning, capital planning, and enterprise architecture.

The Information Security Committee, led by the CISO, with leadership representation from across SED must meet regularly to discuss the information security program, requirements, and risks concerns, as outlined in the Information Security Committee Charter.

- The Deputy Commissioners are responsible for implementing privacy and security policies and practices into the operations of their program offices and the Department, including strategic planning, budget planning, and organization architecture.

3 GOVERNANCE

SED shall develop, implement and maintain an organization-wide privacy and security program to address the confidentiality, integrity and accessibility of SED IT systems and data that support the operations and assets of SED, including those provided or managed by another organization, contractor, or other source.

3.1 ACCEPTABLE USE POLICY, USER ACCOUNT PASSWORD POLICY AND OTHER RELATED DEPARTMENT POLICIES

- Users must comply with NYSED's Information Security Policy, which outlines the responsibilities of all users of SED information systems to maintain the security of the systems and to safeguard the confidentiality of SED information.
- Users must comply with the Acceptable Use of IT Resources Policy in using Department resources.
- Users must comply with the User Account Password Policy.
- All remote connections must be made through managed points-of-entry in accordance with the Data Privacy and Security Guidelines for Remote Work and Telecommuting Policy.

3.2 DATA PRIVACY

- The confidentiality of SED data must be protected and must only be used in accordance with state and federal laws, rules and regulations, and SED policies to prevent unauthorized use and/or disclosure.
- SED's Chief Privacy Officer leads the Data Privacy Governance Board. The Data Privacy Governance Board reviews approves and/or provides guidance to SED program offices when the collection, disclosure, or new processing of personal information protected by law is contemplated.
- Where required by law, personal information, personally identifiable information, shall only be disclosed to third parties pursuant to a written agreement that includes terms and conditions necessary to protect such information.
- It is SED's policy to provide all protections afforded to parents and persons in parental relationships, or students where applicable, required under the Family Educational Rights and Privacy Act, the Individuals with Disabilities Education Act, and the federal regulations implementing such statutes.

3.3 PRIVACY AND SECURITY RISK MANAGEMENT STRATEGY

- SED will have policies and practices in place that identify the risks to the confidentiality, integrity, and accessibility of its IT systems and data, and manage its operations and the actions of its employees and vendors to minimize, mitigate or eliminate identified risk in line with applicable laws, rules and regulations, and industry recommended practices. To aid implementation of this strategy, SED shall:
- Conduct routine penetration tests to identify vulnerabilities that could be exploited by adversaries.
- Develop policies, processes, and procedures to manage and monitor SED's compliance with regulatory, legislative, technical, and organization mandates that protect the confidentiality, integrity, and availability of data.
- Address data privacy requirements and compliance by third-party vendors through its contracting process and must include terms and provisions in its contracts that address the risks to SED IT systems and data.
- Adopt policies and processes to ensure risks to data are identified, assessed, and responded to timely. Establish a process to ensure that applicable policies and procedures that address the protection of data are reviewed for improvements and updates/changes in regulations annually.
- The risk management strategy must be implemented consistently across SED, and must be periodically reviewed and updated, as required, to address organizational changes.

3.4 PRIVACY AND SECURITY RISK ASSESSMENTS

- Whenever there is a significant change to SED's information system or environment of operation, when new systems are implemented, when major modifications are undertaken, when changes in data elements occur, or when a system is migrating or deployed to a third party or to the cloud, SED will perform a risk assessment that assesses impact on privacy of personal information and impact to data security to assess the risk to the privacy of personal information of such changes.
- The risk assessment must capture the data flow (e.g., where the data is coming from, where it is processed/stored, and whom it is shared with). In addition, the risk assessment must state the legal authority for the collection of the data, and records retention schedule covering how long the data must be stored in the information system.
- Risk assessment results must be formally documented and disseminated to appropriate personnel including the system owner, the CIO, CPO, CISO, and other SED stakeholders, as applicable.

4 ASSET MANAGEMENT

SED IT assets deemed critical for SED to achieve its mission and objectives must be identified and managed commensurate with their risk level and importance to the organization.

4.1 PHYSICAL DEVICE INVENTORY (HARDWARE)

- All physical information systems within SED shall be inventoried, and essential information systems identified in accordance with SED's Data Classification Policy.

4.2 SOFTWARE AND APPLICATIONS

- All software platforms and applications within SED shall be inventoried.
- Inventories must include detailed information about the installed software, including the version number and patch level.
- The software/application inventory must be updated periodically, using an automated process where feasible.

4.3 DATA FLOW MAPPING

- An inventory of the types of restricted and confidential data that SED collects, where it is stored, and the third parties that receive it or receive access to it must be maintained. The inventory must document the type of restricted or confidential data collected, the authorization and purpose of collection and external parties to whom it is disclosed, and the authorization and purpose for such disclosure.

5 ACCESS CONTROL

- Access controls shall be implemented on all SED physical and virtual information systems and assets maintained by SED or on behalf of SED, to protect against unauthorized information alteration, loss, denial of service, or disclosure, as outlined in the information security policy.
- SED must establish processes and procedures to ensure that data is protected and only those with a need to know or need to access to perform their duties and/or administrative functions can access the data. Access privileges will be granted in accordance with the user's job responsibilities and will be limited only to those necessary to accomplish assigned tasks in accordance with SED's mission and business functions.

- These duties and/or administrative functions must be captured in the risk assessment for each respective information system that collects, maintains, uses, and/or shares personal information.
- Where technically feasible, users must be provided with the minimum privileges necessary to perform their job duties.

6 AWARENESS AND TRAINING

All SED personnel, volunteers, interns, and contractors with access to SED information systems and/or information must complete data privacy and security awareness training on an annual basis.

7 DATA SECURITY

To protect the confidentiality, integrity, and availability of SED data residing within SED systems, data security and data privacy controls must be incorporated into all aspects of the information systems, including the communications among and with these systems, and with systems external to SED boundaries.

7.1 DATA IN TRANSIT AND AT REST

- All data in transit and at rest containing confidential or restricted information must be encrypted in accordance with the SED Encryption Standard, where technically feasible. Where encryption is not technically feasible, one or more approved compensating control(s) must be adopted that addresses the same risk in accordance with applicable policies, laws, regulations, and standards.
- Systems must implement cryptographic mechanisms to prevent unauthorized disclosure of data and detect changes to data during transmission where technically feasible, unless otherwise protected by appropriate safeguards.
- All SED laptop computers must be secured in accordance with the SED Encryption Standard.
- Removable media must not be used to store confidential or restricted information unless the removable media are encrypted in accordance with the SED Encryption Standard.
- Removable media that is written to must be encrypted in accordance with the SED Encryption Standard.

8 INFORMATION PROTECTION

System protection controls must be established, implemented, and enforced on all essential SED information systems in accordance with SED security standards.

8.1 CONFIGURATION MANAGEMENT

- An enterprise configuration management plan must be developed, documented, and implemented.
- Personnel with configuration management responsibilities must be trained on SED's configuration management process.
- A current baseline configuration of essential systems must be developed, documented, and maintained.
    - Baseline configurations for SED workstations and laptops must be established, and images must be automatically deployed.
    - Server implementations must be deployed from a common baseline image per operating system. Baseline configurations must be reviewed and updated as part of system component installations and upgrades.
- Previous versions of the baseline configuration must be retained to support rollback.

8.2 CHANGE CONTROL

- Proposed system changes must be reviewed and approved prior to implementation. No scheduled changes are permitted outside of the configuration management process. The results of security impact analyses must be considered as part of the change approval process.
- Changes to systems (to include security patches) must be prioritized and implemented in a manner that ensures maximum protection against IT security vulnerabilities and minimal impact on business operations**.**
- If required changes (to include patches) are not applied, an approved risk-based decision must be documented.
- Approved changes (to include patches) must be tested and validated on non-production systems prior to implementation, where technically feasible. System changes must be analyzed to determine potential security impacts prior to change implementation.

8.3 BACKUPS

- Backups of critical SED systems and data must be conducted. The strategy to support system and data recovery must be documented.
- Backup data to be used for disaster recovery efforts must be stored at a secure off-site location.
- The confidentiality, integrity, and availability of backup information must be protected.
- Recovery procedures must be tested at least annually to verify procedure validity, media reliability, and information integrity. The result of the testing must be documented.

8.4 PHYSICAL ENVIRONMENT

- Controls must be implemented to ensure the physical and environmental protection of data and systems.
- Such controls must be commensurate with the level of data being stored, transmitted or processed in the physical location but can include emergency power shutoff, standby power, fire detection/suppression systems, environmental controls and monitoring, and physical access control and monitoring.

8.5 DATA SANITIZATION

- All sanitization and disposal techniques must be performed in accordance with SED's Secure Disposal Standard.
- All media sanitizations must be tracked, documented, and verified.
- Sanitization procedures must be tested.
- Both electronic and hard copy media must be sanitized prior to disposal, transfer, release out of organizational control, donation, or release for reuse, using sanitization techniques and procedures as outlined in the Secure Disposal Standard.
- Personal identifiers must be removed from personal information to make it anonymous before it is provided to third parties who require it for research or before it is published publicly such that the data cannot be used to identify a specific individual.

8.6 RESPONSE PLANNING

- SED's CISO, CIO and CPO have developed an Incident Response Policy and Plan to guide its response to data and cybersecurity incidents. The Incident Response Policy must be employed when an incident occurs.
- The Incident Response Plan must be:
    - Reviewed at least annually and updated to address system/organization changes.
    - Communicated to staff with incident response responsibilities.
    - Protected from unauthorized disclosure or modification.

8.7 VULNERABILITY MANAGEMENT

- A vulnerability management plan for SED systems and information processing environments must be developed and implemented. Systems must be scanned for vulnerabilities and vulnerabilities must be remediated in accordance with an assessment of risk within maximum allowable timeframes.

9 MAINTENANCE

Repairs and maintenance on all hardware and software must be controlled and performed only by approved personnel. Questions about approval will be addressed by the Chief Information Officer. Security commensurate with the sensitivity level of the system data must be implemented to protect data and information systems from unauthorized access or modification.

- All maintenance activities must be approved and monitored by designated system/facility staff.
- To the extent possible, all maintenance activities must be scheduled in advance and approval granted by the impacted parties.
- All software patches and updates must only be deployed after research and testing has been conducted in a development or test environment, where such test or development environments exist. Unless no test or development environment exists, software patch and/or update testing on operational systems is prohibited.
- All systems must be reviewed on a regular basis to ensure that current patches are applied.
- Maintenance tools must be inspected, approved, controlled, and monitored. All media must be checked for malicious code before being introduced to the production environment.
- A process for maintenance personnel authorization must be established and a list of authorized maintenance organization/personnel must be maintained.
- Session and network connections for remote maintenance must be terminated when non-local maintenance is completed.
- Remote maintenance and diagnostic sessions must be audited, and the records reviewed by designated system/facility staff.

9.1 PROTECTION AND MONITORING

SED IT assets must be adequately protected, controlled, and monitored. Security protections commensurate with the sensitivity level of the system data must be implemented to protect SED IT assets from unauthorized access or modification.

9.2 AUDIT

- SED-designated audit logs must be recorded, retained, and available for analysis by authorized personnel to identify unauthorized activity.
- Access to the management of audit functionality must be restricted to authorized personnel only.
- Where technically feasible, audit records must be correlated across different repositories and sources to gain SED-wide situational awareness and enhance the ability to identify suspicious

activity.

- Internal system clocks must be used to generate time stamps for audit records.
- All audit logs must be protected from unauthorized modification, access, or destruction in accordance with the sensitivity of the data stored therein.
- Audit information and tools must be protected from deletion, unauthorized access, and modification.
- Audit logs must be retained for a minimum of 30 days, where technically feasible.
- Audit trails capable of automatically generating and storing security audit records must be implemented on multi-user systems.

9.3 MEDIA PROTECTION

- All information system media (e.g., disk drives, diskettes, internal and external hard drives, portable devices, etc.), including backup media, removable media, and media containing SED information and/or sensitive information must be secured and protected from unauthorized access at all times.
- Access to digital and non-digital media must be restricted to appropriate personnel.
- All media, including backup media, must be stored securely, and transmitted securely to an off-site location in accordance with applicable business continuity and disaster recovery procedures.
- System media must be physically controlled and securely stored until the media are destroyed or sanitized using approved equipment, techniques, and procedures.

9.4 LEAST FUNCTIONALITY

- All IT systems must be configured to provide only essential capabilities.
- Servers must not be used as workstations.
- The use of high-risk functions, ports, protocols, and/or services must be prohibited or restricted, as appropriate.

9.5 COMMUNICATION PROTECTION

- Data privacy and security controls must be incorporated into all aspects of information system and communications, to protect the confidentiality, integrity, and availability of SED information systems, data residing within these systems, and the communications among and with these systems, and with systems external to SED.

10 ANOMALIES & EVENTS

- System controls and processes must be implemented to ensure system and data integrity (i.e., accuracy, completeness, validity, and authenticity of systems and data) is protected at all times. Measures must be taken to prevent, detect, remove, and report malicious code, viruses, worms, and Trojan horses.
- SED must monitor systems to detect events for indicators of potential attacks and attacks, and conduct security testing, training, and monitoring activities associated with SED information systems.
- Security incidents must be tracked and documented.

10.1 BREACH/INCIDENT RESPONSE PLAN

The Department will respond to data privacy and security incidents in accordance with its Incident Response Policy and Plan. The incident response process will determine if there is a breach.

- The Incident Response Policy and Plan establishes a data breach response process and creates an Incident Response Team (IRT) comprised of existing staff members to address data breaches. Together with the CISO, the IRT must assess the potential impact of the incident and develop and execute a response plan consistent with SED established procedures and requirements.
- Employees must report suspected cybersecurity incidents to the Information Security Office and their immediate supervisor or manager. If a critical incident is verified, the CISO must convene a meeting of the IRT and notify senior management.
- The IRT will notify the Chief Privacy Officer where personal, confidential or sensitive information has been accessed by or disclosed to an unauthorized person. Where a breach is confirmed, the CPO will notify senior management and coordinate the process of compliance with notification requirements. SED will comply with legal requirements that pertain to the notification of individuals affected by a breach or unauthorized disclosure of personally identifiable information.
- Communication with the media, executive branch and Board of Regents regarding an incident must be coordinated with the Office of Communications.

11 APPENDIX A: GLOSSARY

Assurance	Measure of confidence that the security features, practices, procedures, and architecture of an information system accurately mediates and enforces the security policy.
Audit Log	A chronological record of information system activities, including records of system accesses and operations performed in a given period.
Audit Record	An individual entry in an audit log related to an audited event.
Audit Trail	A chronological record that reconstructs and examines the sequence of activities surrounding or leading to a specific operation, procedure, or event in a security-relevant transaction from inception to final result.
Authentication	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.
Authenticity	The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator. See *Authentication*.
Availability	Ensuring timely and reliable access to and use of information.
Baseline Configuration	A documented set of specifications for an information system, or a configuration item within a system, that has been formally reviewed and agreed on at a given point in time, and which can be changed only through change control procedures.
Confidential Information	Confidential Information is information that is prohibited from disclosure by law, rules, or regulations or by SED's policies. It includes personally identifiable information and personal information. Access to confidential information is limited to those SED representatives who need such information to carry out their duty. When confidential information is received from another office, the receiving office must accept the responsibility for the confidential information and secure it appropriately.
Confidentiality	Preserving authorized restrictions on data access and disclosure, including means for protecting personal privacy and proprietary information.

Configuration Management	A collection of activities focused on establishing and maintaining the integrity of information technology products and information systems, through control of processes for initializing, changing, and monitoring the configurations of those products and systems throughout the system development life cycle.
Configuration Settings	The set of parameters that can be changed in hardware, software, or firmware that affect the security posture and/or functionality of the information system.
Countermeasures	Actions, devices, procedures, techniques, or other measures that reduce the vulnerability of an information system. Synonymous with security controls and safeguards.
Department	The New York State Education Department. Also known as SED within this document.
Digital Media	A form of electronic media where data are stored in digital (as opposed to analog) form.
Enterprise	An organization with a defined mission/goal and a defined boundary, using information systems to execute that mission, and with responsibility for managing its own risks and performance. An enterprise may consist of all or some of the following business aspects: acquisition, program management, financial management (e.g., budgets), human resources, security, and information systems, information and mission management. See *Organization*.
Enterprise Architecture	A strategic information asset base, which defines the mission; the information necessary to perform the mission; the technologies necessary to perform the mission; and the transitional processes for implementing new technologies in response to changing mission needs; and includes a baseline architecture; a target architecture; and a sequencing plan.
Environment of Operation	The physical surroundings in which an information system processes, stores, and transmits information.
Event	Any observable occurrence in an information system.
External Network	A network not controlled by SED.
Firmware	Computer programs and data stored in hardware - typically in read-only memory (ROM) or programmable read-only memory (PROM) - such that the programs and data cannot be dynamically written or modified during execution of the programs.

Hardware	The physical components of an information system. See *Software* and *Firmware*.
Impact	The effect on organizational operations, organizational assets, individuals, other organizations, or the Nation (including the national security interests of the United States) of a loss of confidentiality, integrity, or availability of information or an information system.
Incident	An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.
Information	Any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual.
Information Resources	Information and related resources, such as personnel, equipment, funds, and information technology.
Information Security	The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.
Information Security Policy	Aggregate of directives, regulations, rules, and practices that prescribes how an organization manages, protects, and distributes information.
Information Security Program Plan	Formal document that provides an overview of the security requirements for an organization-wide information security program and describes the program management controls and common controls in place or planned for meeting those requirements.
Information Security Risk	The risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation due to the potential for unauthorized access, use, disclosure, disruption, modification, or destruction of information and/or information systems.
Information System	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. Note: Information systems also include specialized systems such as industrial/process controls systems, telephone switching and private branch exchange (PBX) systems, and environmental control systems.

Information System Component	A discrete, identifiable information technology asset (e.g., hardware, software, firmware) that represents a building block of an information system. Information system components include commercial information technology products.
Information Technology	Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which: (i) requires the use of such equipment; or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term *information technology* includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources.
Integrity	Guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity.
Internal Network	A network where: (i) the establishment, maintenance, and provisioning of security controls are under the direct control of organizational employees or contractors; or (ii) cryptographic encapsulation or similar security technology implemented between organization-controlled endpoints, provides the same effect (at least with regard to confidentiality and integrity). An internal network is typically organization-owned yet may be organization-controlled while not being organization-owned.
Local Access	Access to an SED information system by a user (or process acting on behalf of a user) communicating through a direct connection without the use of a network.
Malicious Code **Malware**	Software or firmware intended to perform an unauthorized process that must have adverse impact on the confidentiality, integrity, or availability of an information system. A virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code.
Media	Physical devices or writing surfaces including, but not limited to, magnetic tapes, optical disks, magnetic disks, Large-Scale Integration (LSI) memory chips, and printouts (but not including display media) onto which information is recorded, stored, or printed within an information system.
Multifactor Authentication	Authentication using two or more different factors to achieve authentication. Factors include: (i) something you know (e.g., password/PIN); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric).

Network	Information system(s) implemented with a collection of interconnected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices.
Network Access	Access to an information system by a user (or a process acting on behalf of a user) communicating through a network (e.g., local area network, wide area network, Internet).
Nonlocal Maintenance	Maintenance activities conducted by individuals communicating through a network, either an external network (e.g., the Internet) or an internal network.
Non-repudiation	Protection against an individual falsely denying having performed a particular action. Provides the capability to determine whether a given individual took a particular action such as creating information, sending a message, approving information, and receiving a message.
Organization	An entity of any size, complexity, or positioning within an organizational structure (e.g., a state department or, as appropriate, any of its operational elements).
Organizational User	An SED employee or an individual SED deems to have equivalent status of an employee including, for example, contractor, guest researcher, individual detailed from another organization. Policy and procedures for granting equivalent status of employees to individuals may include need-to-know, relationship to SED, and citizenship.
Personally Identifiable Information (PII) or Personal Information (PI)	Information which can be used to distinguish or trace the identity of an individual (e.g., name, social security number, biometric records, etc.) alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual (e.g., date and place of birth, mother's maiden name, etc.).
Potential Impact	The loss of confidentiality, integrity, or availability could be expected to have: (i) a *limited* adverse effect (FIPS Publication 199 low); (ii) a *serious* adverse effect (FIPS Publication 199 moderate); or (iii) a *severe* or *catastrophic* adverse effect (FIPS Publication 199 high) on organizational operations, organizational assets, or individuals.
Public Information	Public Information is information accessible under the Freedom of Information Law and is available to any person, without regard for one's status or interest.
Records	The recordings (automated and/or manual) of evidence of activities performed or results achieved (e.g., forms, reports, test results), which serve as a basis for verifying that SED and the information system are performing as intended. Also used to refer to units of related data fields (i.e., groups of data fields that can be accessed by a program and that contain the complete set of information on particular items).

Remote Access	Access to a SED information system by a user (or a process acting on behalf of a user) communicating through an external network (e.g., the Internet).
Remote Maintenance	Maintenance activities conducted by individuals communicating through an external network (e.g., the Internet).
Restricted Information	Restricted Information is information that is not public information but can be disclosed to or used by SED representatives to carry out their duties, so long as there is no legal bar to disclosure. Information may also be accessible to a person who is the subject of the information under the Personal Privacy Protection Law.
Risk	A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence. Information system-related security risks are those risks that arise from the loss of confidentiality, integrity, or availability of data or information systems and reflect the potential adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.
Risk Assessment	The process of identifying risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system. Part of risk management incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place. Synonymous with risk analysis.
Risk Management	The program and supporting processes to manage information security risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, and includes: (i) establishing the context for risk-related activities; (ii) assessing risk; (iii) responding to risk once determined; and (iv) monitoring risk over time.
Safeguards	Protective measures prescribed to meet the security requirements (i.e., confidentiality, integrity, and availability) specified for an information system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices. Synonymous with security controls and countermeasures.

	Actions taken to render data written on media unrecoverable by both ordinary and, for some forms of sanitization, extraordinary means.
Sanitization	Process to remove information from media such that data recovery is not possible. It includes removing all classified labels, markings, and activity logs.
Security	A condition that results from the establishment and maintenance of protective measures that enable an enterprise to perform its mission or critical functions despite risks posed by threats to its use of information systems. Protective measures may involve a combination of deterrence, avoidance, prevention, detection, recovery, and correction that should form part of the enterprise's risk management approach.
Security Control	A safeguard or countermeasure prescribed for an information system or an organization designed to protect the confidentiality, integrity, and availability of its information and to meet a set of defined security requirements.
Security Functionality	The security-related features, functions, mechanisms, services, procedures, and architectures implemented within organizational information systems or the environments in which those systems operate.
Security Functions	The hardware, software, and/or firmware of the information system responsible for enforcing the system security policy and supporting the isolation of code and data on which the protection is based.
Security Impact Analysis	The analysis conducted by an organizational official to determine the extent to which changes to the information system have affected the security state of the system.
Security Incident	See *Incident*.
Security Plan	Formal document that provides an overview of the security requirements for an information system or an information security program and describes the security controls in place or planned for meeting those requirements. See *System Security Plan* or *Information Security Program Plan*.
Security Policy	A set of criteria for the provision of security services.
Security Requirement	A requirement levied on an information system or an organization that is derived from applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, procedures, and/or mission/business needs to ensure the confidentiality, integrity, and availability of information that is being processed, stored, or transmitted. Note: Security requirements can be used in a variety of contexts from high-level policy-related activities to low-level implementation-related activities in system development and engineering disciplines.

Security Service	A capability that supports one, or more, of the security requirements (Confidentiality, Integrity, Availability). Examples of security services are key management, access control, and authentication.
Security-Relevant Information	Any information within the information system that can potentially impact the operation of security functions or the provision of security services in a manner that could result in failure to enforce the system security policy or maintain isolation of code and data.
SED IT Assets	SED information systems and communication networks, whether owned, leased or rented by SED, and the information stored, processed, and produced on or by these systems and networks.
Software	Computer programs and associated data that may be dynamically written or modified during execution.
Spam	The abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages.
Spyware	Software that is secretly or surreptitiously installed into an information system to gather information on individuals or organizations without their knowledge; a type of malicious code.
Subsystem	A major subdivision or component of an information system consisting of information, information technology, and personnel that performs one or more specific functions.
System	See *Information System*.
Threat	Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.
Threat Assessment	Formal description and evaluation of threat to an information system.
Threat Source	The intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally trigger a vulnerability. Synonymous with threat agent.
User	Individual authorized to access an information system.
Vulnerability	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

Vulnerability Analysis	See *Vulnerability Assessment*.
Vulnerability Assessment	Systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.

NEW YORK STATE EDUCATION DEPARTMENT Information Security Office (ISO) 89 Washington Avenue Albany, NY 12234	**NYSED ISO STANDARD** Encryption Standard **No: SECS7-V:5.0 (REV 11/20/19)**
Issued By: NYSED Chief Information Security Officer	**Owner:** NYSED Information Security Office

1.0 Purpose and Benefits of the Standard

Encryption is a cryptographic operation that is used to enhance security and protect the Department's electronic data by transforming readable information (a.k.a. 'plaintext') into unintelligible information (a.k.a. 'ciphertext'). Encryption is an effective tool in mitigating the threat of unauthorized access to data.

The benefit to the Department will be an enhanced security of Departmental information using encryption.

2.0 Scope

This standard applies to all Department information in any electronic form or format, transmitted or stored on any Department system, device or media, including laptops, desktops, servers, network devices, portable storage devices, backup media, etc. This standard applies to all individuals storing, accessing, or working with sensitive information in any way, including Department employees, contractors, consultants, interns, or any other user who may have access to Department data and information.

It is the responsibility of users to read and understand this standard and to conduct their activities in accordance with its terms. In addition, users must read and understand the NYSED Information Security Policy and its associated standards.

3.0 Information Statement

The need for encryption of information is based on its classification, risk assessment results, and use case.

Attention must be given to the regulations and national restrictions (e.g. export controls) that may apply to the use of cryptographic techniques in different parts of the world. The U.S. Government restricts the export, disclosure, or release of encryption technologies to foreign countries or foreign nationals, including "deemed exports" to foreign nationals within the United States (excluding those foreign nationals with permanent resident visas (i.e. Green Cards), U.S. citizenship, or 'protected person' status). For questions or concerns, please contact Department Counsel and Legal Services.

Encryption products for confidentiality of data at rest and data in transit must incorporate Federal Information Processing Standard (FIPS) approved algorithms for data encryption at a minimum of 128-bit strength. Minimum key length for digital signatures and public key encryption is 2048. Hashing functions must have a minimum key length of 256. Approved algorithms are contained in Appendix A. Use of outdated, cryptographically broken, or proprietary algorithms is prohibited.

Due to the prevalence of incorrectly implemented cryptography, encryption products must have FIPS 140 (Security Requirements for Cryptographic Modules) validation and be operated in FIPS mode. Refer to Appendix B – Guidance in Selecting FIPS 140 Validated Products for further information.

Electronic information used to authenticate the identity of an individual or process (i.e. PIN, password, or passphrase) must be encrypted when stored, transported, or transmitted. This does not include the distribution of a one-time use PIN, password, passphrase, token code, etc., provided it is not distributed along with any other authentication information (e.g. along with the userid).

A system's security plan must include documentation to show appropriate review of encryption methodologies and products. This will demonstrate due diligence in choosing a method or product that has received substantial positive review by reputable third-party analysts.

3.1 Data in Transit

Encryption is required for data in transit in the following situations:

1. When electronic Personal, Private, or Sensitive Information (PPSI) or Personally Identifiable Information (PII) is transmitted (including, but not limited to, e-mail, File Transfer , instant messaging, e-fax, Voice Over Internet Protocol (VoIP), etc.).
2. When encryption of data in transit is prescribed by law or regulation.
3. When connecting to the Department's internal network(s) over a wireless network.
4. When remotely accessing the Department's internal network(s) or devices over a shared (e.g. Internet) or personal (e.g. Bluetooth, infrared) network. This does not apply to remote access over a Department managed point to point dedicated connection.
5. When data is being transmitted with a Department public facing website and/or web services, they are required to utilize Hypertext Transfer Protocol Secure (HTTPS) in lieu of Hypertext Transfer Protocol (HTTP). Department public facing websites must automatically redirect HTTP requests to HTTPS websites. Minimum browser support is listed in Appendix C.

Appropriate encryption methods for data in transit include, but are not limited to, Transport Layer Security (TLS) 1.2 or later, Secure Shell (SSH) 2.0 or later, WIFI Protected Access (WPA) version 2 or later (with WIFI Protected Setup disabled) and encrypted Virtual Private Networks (VPNs). Components should be configured to support the strongest cipher suites possible. Ciphers that are not compliant with this standard must be disabled. Applications which transmit passwords or other sensitive information in clear text, such as Telnet or File Transfer Protocl (FTP), are prohibited. Secure alternatives such as SFTP, FTPS, SSH, etc. must be used. Email must not be used for automated, regularly scheduled transmissions of sensitive information, secure electronic transfer protocols or similarly compliant software should be used.

3.2 Data at Rest

Encryption means methods of rendering personally identifiable information unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified or permitted by the Secretary of the United States department of health and human services in guidance issued under Section 13402(H)(2) of Public Law 111-5.

Encryption is required for data at rest, as follows:

1. For the systems listed below:

a. datData stores (including, but not limited to, databases, file shares) that contain Department PPSI and PII;
b. All mobile devices, whether Department issued or third party, that access or contain any Department information; and
c. All portable storage devices containing any Department information.

2. When electronic PPSI and PII is transported or stored outside of a Department facility.

Full disk encryption is required for all Department issued laptops that access or contain Department information.

To mitigate attacks against encryption keys, when outside of Department facilities, Department laptops and third-party laptops that access or contain Department PPSI and PII must be powered down (i.e. shut down or hibernated) when unattended.

The Department must have a process or procedure in place for confirming devices and media have been successfully encrypted using at least one of the following, listed in preferred order:

1. Automated policy enforcement;
2. Automated inventory system; or
3. Manual recording keeping.

3.3 Encryption Key Requirements

Effective key management is the crucial element for ensuring the security of any encryption system. Department key management must minimally meet these controls.

- Key management should be fully automated (so personnel do not have the opportunity to expose a key or influence the key creation).
- Keys must be securely distributed and stored, (e.g. keys in storage and transit must be encrypted, access to keys must be limited to individuals who have a business need, etc.).
- Unencrypted keys must not be stored with the data that they encrypt.
- Compromise of a cryptographic key would cause all information encrypted with that key to be considered unencrypted. If a compromise has been discovered a new key must be generated and used to continue protection of the encrypted information. Specific circumstances should be evaluated to determine if a breach notification is required. See the NYSED Cybersecurity Incident Response Policy for additional details.
- Encryption keys and their associated software products must be maintained for the life of the archived data that was encrypted with that product.

3.4 Digital Certificate Requirements

- Only trusted third party certificate authorities (CA) are allowed for Internet facing systems and applications. The trusted CA must be included in the list of trusted authorities in commonly used web browsers.
- The use of self-signed certificates is prohibited for Internet facing systems or applications unless they are used for development and testing systems, which have no sensitive information, are segregated from the production network and resources, and they are prohibited from connecting to external resources.

- Administrators must track certificate expiration dates to ensure that applications and systems are available as required.

3.5 Wireless (WIFI) Communications

- All Department wireless networks must be encrypted. See the NYSED Wireless Network Security Standard for additional details.
- The strongest form of wireless authentication permitted by the client device must be used. For most devices and operating systems, WPA2-Enterprise with 802.1x/EAP-PEAP must be used.
- Client devices that do not support WPA2 should be secured using VPN technology such as IPSEC where allowed by the client device.

4.0 Compliance

This standard shall take effect upon publication. The Information Security Office (ISO) shall review the standard at least every two years to ensure relevancy. To accomplish this assessment, the ISO may issue, from time to time, requests for information to other office departments, which will be used to develop any reporting requirements as may be requested by the Department Chief Information Security Officer, the Board of Regents, or Legislative entities.

If compliance with this standard is not feasible or technically possible, or if deviation from this standard is necessary to support a business function, the office shall request an exception through the NYSED Information Security Exception Standard process.

Any violation of this standard may subject the user to disciplinary action up to and including termination. The Department will review alleged violations of this standard on a case-by-case basis and pursue recourse, as appropriate.

5.0 Definitions of Key Terms

Advanced Encryption Security (AES): A specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST). Data stored with AES cannot be decrypted without the key.

Digital Certificate: A form of electronic credentials for the Internet. Digital certificates are used to verify that a user sending a message is who he or she claims to be.

Encryption: A technique used to protect the confidentiality of information. The process transforms ("encrypts") readable information into unintelligible text through an algorithm and associated cryptographic key(s).

File Transfer Protocol (FTP): A standard network protocol used to transfer files from one host to another host over a TCP-based network, such as the Internet.

Internet Protocol Security (IPSEC): A framework of open standards for helping to ensure private, secure communications over Internet Protocol (IP) networks using encryption.

Key: A cryptographic key is a string of bits used by a cryptographic algorithm to transform plain text into cipher text or vice versa.

Key Management: The processes and procedures for providing the generation, distribution, tracking, control, and destruction for all cryptographic keys and their associated certificates.

Mobile Device: A computer device in a small form factor that has at least one network connection interface, non-removable and/or removable storage, and is portable, including but not limited to smartphones, Personal Digital Assistants (PDAs), tablets, laptops, smart watches, and wearable devices.

Portable Storage Device: A storage device that is capable of being physically transported, including but not limited to USB/flash drives/thumb drives, external hard drives, tapes, CDs, DVDs, and cameras.

Secure File Transfer Protocol: SFTP, or secure FTP, is a program that uses SSH to transfer files. Unlike standard FTP, it encrypts both commands and data, preventing passwords and sensitive information from being transmitted in the clear over the network.

Secure Shell (SSH) - A network protocol that establishes an encrypted tunnel between an SSH client and a server.

Transport Layer Security (TLS) - A network protocol for transmitting private documents via the Internet. Websites (URLs) that require an TLS connection start with "*https:"* instead of "*http:*".

Virtual Private Network (VPN) - Virtual Private Network. A network which emulates a private network, although runs over public network lines and infrastructure.

Wireless Fidelity (**Wi-Fi) -** A mechanism that allows electronic devices to exchange data wirelessly.

Wi-Fi Protected Access 2 (WPA2) - A security protocol for wireless networks that provides data protection and network access control.

6.0 ISO Contact Information

Submit all inquiries and requests for future enhancements to the standard owner at:

NEW YORK STATE EDUCATION DEPARTMENT
Information Security Office
Website: http://atwork.nysed.gov/iso/
Email: infosec@nysed.gov

7.0 Review Schedule and Revision History

Date	Description of Change	Reviewer
3/12/2019	DRAFT, Updated ISO contact information as well as Section 1 and 4.	Marlowe Cochran, Chief Information Security Officer
8/9/2019	Reviewed, Remove pre-boot option, update file transfer language	ITS, CPO, CISO
11/20/2019	Updated Contact Information	Marlowe Cochran, Chief Information Security Officer

12/5/2019	Original Standard Release	Marlowe Cochran, Chief Information Security Officer

8.0 Related Documents

- NYSED Acceptable Use of Information Technology (IT) Resources Standard
- NYSED Information Security Policy
- NYSED Cybersecurity Incident Response Policy
- NYSED Wireless Network Standard
- Secretary of the United States department of health and human services guidance issued under Section 13402(H)(2) of Public Law 111-5

9.0 Appendix A – Approved Algorithms

Algorithm	Minimum Key Length	Use Case
AES	128	Data Encryption
RSA	2048	Digital Signatures Public Key Encryption
ECDSA	256	Digital Signature Public Key Encryption
SHA	256	Hashing

10.0 Appendix B – Guidance for Selecting FIPS 140 Validated Products

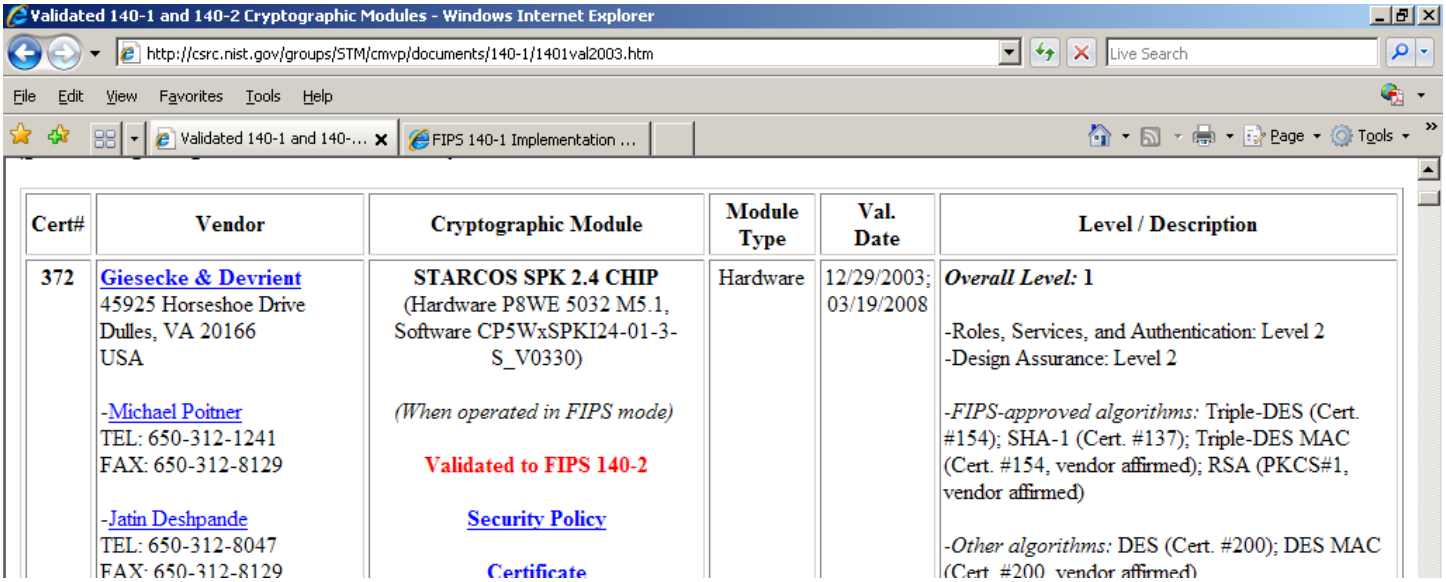
All government agencies that use cryptographic-based systems to protect Personal, Private, or Sensitive Information (PPSI) or Personally Identifiable Information (PII), need to have a minimum level of assurance that the product's stated security claim is valid.

On July 17, 1995, the National Institute of Standards and Technology (NIST) established the Cryptographic Module Validation Program (CMVP) that validates cryptographic modules to Federal Information Processing Standards (FIPS) cryptography based standards.

Historically, over 48% of cryptographic modules that have undergone FIPS validation had security flaws that were corrected during testing. In other words, without validation, users would have had only a 50-50 chance of buying correctly implemented cryptography.

The list of FIPS validated cryptographic modules can be found on the NIST web site at http://csrc.nist.gov/groups/STM/cmvp/validation.html. The list can be searched by vendor or by year of validation.

Figure 1: Screenshot of NIST CMVP Validation List for All Years



It is important to note that items on this list are cryptographic modules which may either be an embedded component of a product or application, or a complete product in and of itself. In addition, it is possible that vendors who are not found on this list might incorporate a validated cryptographic module from this list into their own products.

When selecting a product from a vendor, verify that the application or product that is being offered is either a validated cryptographic module itself (e.g. full disk encryption solution, SmartCard) or the application or product uses an embedded validated cryptographic module (toolkit, etc.) by confirming the module's validation certificate number. Ask the vendor to supply a signed letter stating their application, product, or module is a validated module or incorporates a validated module which provides all the cryptographic services in the solution, and references the module's validation certificate number. This number can be checked against the CMVP validation list. If the information does not agree, the vendor is not offering a validated solution.

Figure 2: Certificate Number of NIST CMVP Validation List

1040	Cisco Systems, Inc. 170 West Tasman Drive San Jose, CA 95134 USA -Global Certification Team TEL: **CST Lab:** NVLAP 200427-0	**Cisco 3825 and Cisco 3845 Integrated Services Routers** (Hardware Versions: 3825 and 3845; Firmware Versions: 12.4(15)T3[1] and 12.4(15)T10[2]) *(When operated in FIPS mode)* **Validated to FIPS 140-2** Security Policy Certificate	Hardware	10/14/2008; 08/28/2009; 10/23/2009; 05/28/2010; 02/23/2012	***Overall Level:* 2** *-FIPS Approved algorithms:* A (Certs. #50, #436 [1] and #696 (Certs. #379 [1] and #576 [2]); DES (Certs. #210, #683 [1] an *-Other algorithms:* Diffie-Hell provides 80 or 96 bits of encry key establishment methodolog compliant less than 112 bits of DES Multi-chip standalone "The Cisco 3800 Series feature simultaneous services at wire s routers offer embedded encryp

Be aware that vendors may sometime make invalid conformance claims such as:

- The module has been designed for compliance to FIPS 140-x.
- The module has been pre-validated and is on the CMVP pre-validation list.
- The module will be submitted for testing.
- The module has been independently reviewed and tested to comply with FIPS 140-x.
- The module meets all the requirements of FIPS 140-x.
- The module implements FIPS Approved algorithms; including having algorithm certificates.
- The module follows the guidelines detailed in FIPS 140-x.

A cryptographic module does not meet the requirement or conform to the FIPS standard unless a reference can be made to the validation certificate number.

Users must also be cognizant of the version number of the validated cryptographic module and, for software products, the operating system that it has been tested on. Only the version numbers listed in the Cryptographic Module column of the CMVP list are FIPS validated and only when run on the operating systems listed in the Level/Description column.

Figure 3: Version Number and Operating Systems on NIST CMVP Validation List

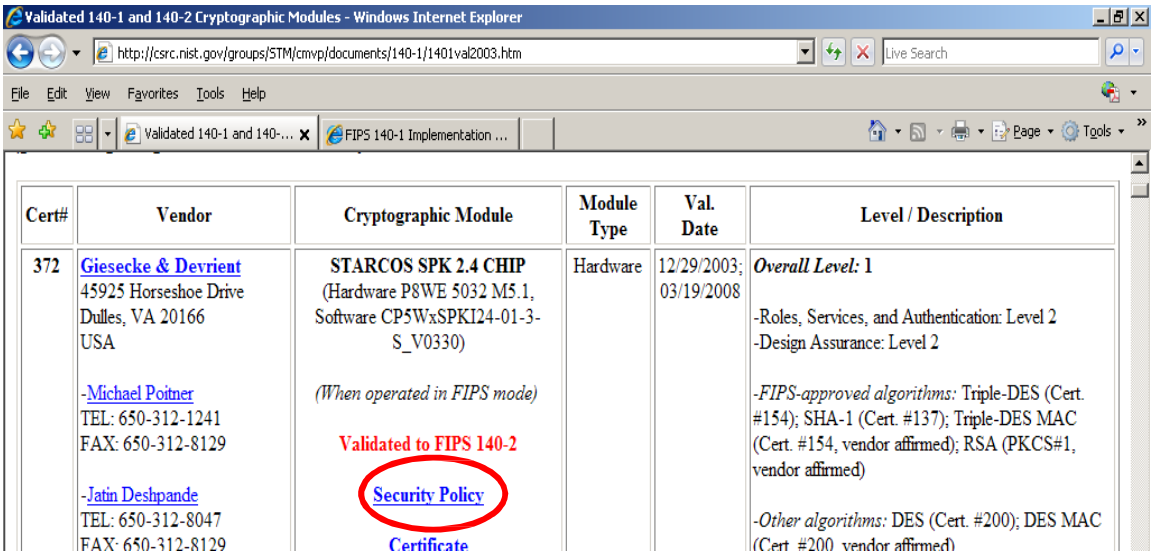
1010	Microsoft Corporation One Microsoft Way Redmond, WA 98052-6399 USA -Dave Friant TEL: 425-704-7984 FAX: 425-936-7329 **CST Lab:** NVLAP 200427-0	**Windows Server 2008 Enhanced Cryptographic Provider (RSAENH)** (Software Versions: 6.0.6001.22202 and 6.0.6002.18005) *(When operated in FIPS mode with Code Integrity (ci.dll) validated to FIPS 140-2 under Cert. #1006 operating in FIPS mode)* **Validated to FIPS 140-2** Security Policy Certificate	Software	08/15/2008; 07/24/2009	***Overall Level:* 1** -Operational Environment: Tested as meeting Level 1 with Microsoft Windows Server 2008 (x86 Version); Microsoft Windows Server 2008 (x64 version); Microsoft Windows Server 2008 (IA64 version) (single-user mode) *-FIPS Approved algorithms:* AES (Cert. #739); HMAC (Cert. #408); RNG (SP 800-90, vendor affirmed); RSA (Certs. #353 and #355); SHS (Cert. #753); Triple-DES (Cert. #656) *-Other algorithms:* DES; MD2; MD4; MD5; RC2; RC4; RSA (key wrapping; key establishment methodology provides between 112 and 150 bits of encryption strength; non-compliant less than 112 bits of encryption strength)

FIPS Mode

Many validated products have the capability to operate in FIPS mode, as well as non-FIPS mode. Operating in FIPS mode will ensure that the module uses only FIPS approved encrypted algorithms.

Vendors provide a "Security Policy" as part of their module/product validation. This "Security Policy" can be found under the Cryptographic Module column on the CMVP list. The "Security Policy" will provide information on how to configure the module in a FIPS mode of operation and how the module functions to meet the FIPS requirements.

Figure 4: Security Policy on NIST CMVP Validation List



Modules in Process

NIST maintains a Modules in Process list. Inclusion on the list is at the option of the vendor. Posting on this list does not imply a guarantee of final FIPS validation. Therefore, SEs that deploy a module before it is validated incur a level of risk in that the module may never be validated, or the version submitted for testing is not the version that is validated.

11.0 Appendix C – Minimum Browser Support

Browser	Supported Version
Google Android OS Browser	Android 6.0-6.0.1, 7.0-7.1.0 and higher
Google Chrome	49 and higher
Mozilla Firefox	49 and higher
Microsoft Internet Explorer	IE 11 or higher
Microsoft Edge	Edge 12 or higher

Microsoft Edge	Edge 13 for Windows 10 Mobile v1511 or higher
Microsoft Internet Explorer Mobile	None – No support for Windows Phone 8.1 or below
Opera Browser	37 or higher
Apple Safari	10 or higher & macOS 10.12 or higher
Apple Safari Mobile	10 or higher & ISO 10 or higher

Firewall Policy

Information Bulletin Vol. 3, No. 1, January 22, 1999

1.0 Background & Purpose

A firewall centrally controls access between a trusted network such as SED's internal network and an untrusted network such as the Internet, NYT or OGS MAN. It acts as a "gatekeeper" that can provide the following functionality:

- Block unwanted traffic from an untrusted network.
- Reroute incoming traffic to a specific system.
- Hide vulnerable systems that can not easily be secured from the Internet.
- Log traffic to and from SED's internal network and the Internet.
- Hide internal "hacker-helpful" information such as system names, network devices and internal USERIDs from being seen outside SED's network.
- Provide more robust authentication (encryption, passwords, etc.) than internal systems may be able to do.

Without a firewall in place, all desktop computers, servers and any other equipment connected to the network are vulnerable to an attack from an outside network. Although passwords protect these systems, userid/password authentication provides only a minimal amount of security. A firewall provides an additional layer of security by either blocking access to a server or requiring authentication before access to SED's internal network is granted.

> *Think of it this way: If the roads to get to your home represented the network and your home represents a server on the network, then anyone can walk right up to your front door and try to get in. (And, by the way, the physical key to your house provides better security than a password.) A firewall would be like having a guard at the entrance to your street who will only allow in the specific visitors you authorize. Everyone else would be turned away.*

Implementing a firewall is more than just setting up the hardware and software. The key part of setting up a firewall is establishing a policy that defines the services that may be accessed, by whom and under what constraints. The purpose of this document is to establish that policy for SED's network.

> *It should be noted that the firewall policy is only a part of an overall security strategy and is highly dependent on other policies. There is an inherent conflict between security and convenience, which may lead to security holes between two seemingly unrelated policies. For example, a policy that allows modems on desktop computers provides a means to circumvent the firewall protection.*

2.0 General Policy

Since convenience and security are mutually exclusive, we want to try to strive towards making it easy for SED staff to continue to access sites and information outside our internal network. However, we want to be sure that outside users can only get to information and systems that we want them to access within our network. Therefore the policy will differentiate between outbound traffic and inbound traffic.

2.1 Outbound Traffic

In general, SED staff will have access from a computer connected to SED's internal network to any site on the Internet, NYT and OGS MAN using SED-approved software and gateways. SED reserves the right to block accesses to specific sites that have no SED-related business value or contain illegal content. Requests to block specific sites should be sent to SED's Information Security Officer (ISO) along with the reasons for blocking access to the site.

The ISO can periodically monitor the firewall logs and audit trails to ensure compliance with SED's Internet Acceptable Use Policy (see "Policies & Procedures" on ATWORK.NYSED.GOV for information on the Acceptable Use Policy.)

> *Note on privacy: The firewalls only log information about the originating and destination network addresses and authentication information. They do not log anything about the content of the information being sent or received.*

2.2 Inbound Traffic

By default, all access to SED's internal network by users from an external network will be blocked at the firewall except to

specific services as outlined in Attachment 1. Once the firewall is installed, requests for additional exceptions must be approved by the ISO. Whenever feasible, servers that provide information to external users will be connected to an SED-owned network that is physically separated from the SED internal network but is transparently accessible from both the internal network and from the Internet.

> *In firewall terminology this separate network is referred to as the Demilitarized Zone (DMZ). Access to the DMZ from either the Internet or internal network requires traffic to pass through the firewall where it can be monitored, audited or restricted as needed.*

Certain services that provide "hacker-useful" information or are by their nature hard to secure will not be allowed through the firewall to our internal network. These services include:

- Unix ‘r’ commands such as rlogin, rcp, rsh, etc., which are designed to let users execute commands on remote systems typically do not support authentication or encryption and are therefore easy to exploit.
- Unix remote printing protocols (lp and lpr) which allow you to use printers attached to other hosts fall into the same category as above since lp uses the rsh function.
- Network News Transfer Protocol (NNTP) is used to support discussion lists and Usenet news groups and has been the target of recent attacks. NNTP servers should reside in the DMZ rather than inside SED’s internal network.
- Network File System (NFS) allows disk drives to be accessed by other users across the network. Unfortunately it uses very weak authentication and is not considered safe to use across an untrusted network.
- Finger and Whois fall into the same category. Both are designed to provide information to other users about a system or another user which can also be helpful to someone attempting an attack on a system.

In addition, external network users should not be allowed to use anonymous FTP inside SED’s internal network. Anonymous FTP servers should be located in the DMZ if access is needed from the Internet, NYT, etc.

3.0 Firewall Administration

The ITS Network Unit will be responsible for firewall administration and support. Requests to allow new services or users through the firewall should be submitted to the ISO for authorization. Upon granting authorization, the ISO will forward the request to the Network Unit for implementation. Under normal circumstances, turn around time will be 5 business days.

REFERENCES

1. "Internet Security Policy: A Technical Guide", National Institute of Standards and Technology (NIST), June 1998
2. "Getting Started with Firewall-1", Sun Microsystems, April 1997
3. "Technology Policy 96-8", Governor’s Office for Technology, May 1996
4. "Technology Policy 96-11", Governor’s Office for Technology, November 1996
5. "Technology Policy 97-1", Governor’s Office for Technology, January 1997
6. "Network Security: Beyond the Firewall", Government Technology Conference Seminar, Nortel (formerly Bay Networks, Inc.), October 1998
7. Governor’s Office for Technology Security Steering Committee
8. Unified Technologies, Inc.

NEW YORK STATE EDUCATION DEPARTMENT Information Security Office (ISO) 89 Washington Avenue, Albany, NY 12234	**NYSED ISO POLICY** Information Security Policy **No: SECP1 - V:5.0: (Rev 12/2/2020)**
Issued By: NYSED Chief Information Security Officer	**Owner:** NYSED Information Security Office

1.0 Purpose

Information security is of the utmost importance to the NYS Education Department (SED); in a collaborative world dependent upon shared information, it is essential that the NYS Department of Education implement an information security to protect and maintain confidentiality; integrity, and availability of all its data created, received or gathered by SED; and to its systems and information technology resources (IT resources).

NYSED Information Security Policy outlines the mandatory minimum data security requirements and responsibilities of all employees, volunteers, interns, consultants, and third-party contractors ("Users") of SED who has access to data and systems to maintain the security of these systems and to safeguard the confidentiality of SED information.

2.0 Scope

Understanding the risks, threats, costs and incidents associated with securing Department Information is a shared responsibility.

This Policy applies to all SED Users that receive sensitive, restricted, or confidential information, or have access to SED's data, systems and data assets are responsible for ensuring the protection of Department data and IT resources and assets.

The Policy also, applies to all SED physical and virtual systems, and communication networks, whether owned, leased or rented by SED, and the information stored, processed, and produced on or by these systems, networks, or software applications.

3.0 Functional Responsibilities

Security is a shared responsibility

This policy defines the roles and responsibilities of SED's Executive Leadership, CIO, CISO, CPO, users, and third-party.

The Chief Information Officer (CIO):

1. Supporting security by providing clear direction and consideration of security controls in the data processing infrastructure and computing network(s) which support the information owners;
2. Advocate resources needed to maintain a level of information security control consistent with this policy;
3. Identifying and implementing all IT processes, policies and controls relative to security requirements defined by SED's business and this policy;
4. Assist with implementing the proper controls for information owned by SED's classification designations;
5. Providing training to appropriate technical staff on secure operations (e.g., secure coding, secure configuration);
6. Fostering the participation of information security and technical staff in protecting information assets, and in identifying, selecting and implementing appropriate and cost-effective security controls and procedures; and
7. Ensuring IT requirement that the business continuity and disaster recovery plans are met.

The Chief Privacy Officer (CPO):

1. Shall promulgate regulations, establishing data security and privacy policies and standards pertaining to student, teacher, and principal data for educational agencies;
2. Annually report to the Board of Regents on data privacy and security activities and progress for educational agencies, the number and disposition of reported breaches;
3. The CPO chairs the SED's Data Privacy Governance Committee and participates in SED's Information Security Committee Committees.

The Chief Information Security Officer (CISO):

1. Is responsible for security functions, including assisting in the interpretation and application of this policy, including approving exceptions;
2. Provides in-house expertise as security consultants as needed;
3. Develops SED's security program and strategy, including measures of effectiveness;
4. Establishes and maintains enterprise information security policy and standards; and
5. Monitors external sources for indications of compromises (IOC), defacements, etc.; and reporting of incidents.

Manager:

1. A person who supervises/manages other personnel or approves work on behalf of SED.
2. Are required to notify appropriate SED point of contact (POC) of any personnel transfers or separations within 48 hours of transfer/separation.

Office of Human Resources Management (OHRM):

1. The Office of Human Resources Management will be responsible for the onboarding and offboarding of personnel;

2. OHRM will be responsible for personnel issues arising from intentional or repeated violations of SED information security policies and procedures;
3. OHRM will take appropriate administrative action, including formal discipline and/or legal action. The actions taken by OHRM may range from counseling and suspension of user access, to discipline, which can include suspension, termination or legal action for more serious violations.

Users:

A user is a staff, volunteer, contractor, vendor, consultants, intern, or person working for SED in any capacity or through any other augmentation to SED staffing levels.

Users are responsible for the following:

1. Understanding the baseline information security controls necessary to protect the confidentiality, integrity and availability of information entrusted to State Entities;
2. Protecting State information and resources from unauthorized use or disclosure;
3. Protecting personal, private, sensitive information from unauthorized use or disclosure;
4. Abiding by NYSED Policy, ISO-P14-001, Acceptable Use of Information Technology Resources; and
5. Reporting suspected information security incidents or weaknesses to the appropriate manager and ISO/designated security representative.

4.0 POLICY TEXT

I. Acceptable Use Policy

Acceptable use of IT resources and effective security require the participation and support of the users. Unacceptable use exposes the Department to potential risks including malware attacks, compromise of network systems and services, and legal liability.

Therefore users must comply with the Acceptable Use of IT Resources Policy when using Department resources. This policy reinforces the responsibility to protect information and utilize only sanctioned technology. All users of information technology resources must comply with Department policies, standards, procedures, and guidelines, as well as any applicable Federal, State and local laws, including copyright laws and licensing agreements.

Please go to (Acceptable Use IT Resources Policy) for more information regarding the acceptable use of Information Technology (IT).

II. User Account Password Policy

Passwords are an important part of the Department's information security program. Strong passwords applied to Department Information Technology (IT) resources reduce the risk of unauthorized access to electronic information. The purpose of this policy is to establish a standard for the creation of strong

passwords, the protection of those passwords, and the frequency of changing these passwords. Users must comply with the User Account Password Policy.

Please go to the (User Account Password Policy) for more information regarding user passwords.

III. User Accounts

Each User will have to have a unique user account to distinguish that user from other users in accordance with NYSED User Account Policy.

Access must be approved by the appropriate role, and the User must complete all required training prior to receiving access.

Departments/business units must assign privileged access based on job functions and must include clear instruction for appropriate use.

IV. Data Privacy

Maintaining the privacy of the various types of sensitive, confidential, personal or personally identifiable data that SED collects, processes and stores is a critical responsibility that is taken seriously. SED will protect its data, systems and data assets in accordance with applicable state and federal laws and regulations and SED's policies.

Please go to Data Privacy and Security (Laws and Regulations) for more information regarding the Data Privacy and Security Policy.

Associated Standards: NYSED Data Privacy and Security Policy; Family Educational Rights and Privacy Act (FERPA); Parents-bill-of-rights.pdf; report-improper-disclosure; Student-data-privacy/collected-data-elements.pdf.

V. Data and System Security

SED will adopt physical, technical and administrative controls necessary to protect its data, systems and assets against intentional or unintentional loss of confidentiality, integrity, or availability.

All NYSED systems must have appropriate security controls to ensure they are protected against malicious actors or threats.

Access privileges to data and systems will be granted in accordance with the user's job responsibilities and will be limited only to those necessary to accomplish assigned tasks in accordance with State Entity missions and business functions (i.e., least privilege). Accounts will be removed, and access will be denied for all those who have left the agency or moved to another department.

An overview of the security requirements, but not all inclusive, for physical and virtual systems and the security controls in place or planned for meeting those requirements are below.

Various controls, such as: change management, configuration management, vulnerability management, and incident response processes, plans and procedures must be established, implemented, and enforced on all essential SED information systems in accordance with SED security standards.

Associated standards: nys-s14-008_secure_configuration NYSED_SECS6-V4_SecureDisposalStandard, and NYS-S14-003, Information Security Controls.

VI. Telecommuting Remote Access Policy

NY State Education Department (SED or Department) employees that work from home using agency SED laptops, cell phones or tablets, or their own personal devices to check their email, review documents or view or and/or connect remotely to Department systems and data must protect the privacy and security of Department data and systems. It is every employee's responsibility to protect Department data, especially data designated as Personal, Private, Restricted, or Confidential Information.

All remote connections must be made through managed points-of-entry in accordance with the Data Privacy and Security Guidelines for Remote Work and Telecommuting Remote Access Policy and the Remote Access Request Form.

Please go to (Data Privacy and Security Guidelines for Telecommuting) for more information regarding telecommuting.

Associated standards: NYSED password policy and guidelines, NYSED_SECF3-V1_Secure_Remote_Access_Request_Form, Data Privacy and Security Guidelines for Remote Work and Telecommuting Remote Access Policy, NYSED Responsibilities of the User, and NYS-P14-001 Acceptable Use of Information Technology (IT) Resources Policy.

VII. Data Classification and Handling

Data classification is the basis for identifying an initial baseline set of security controls for data, systems physical or virtual, and evaluation of retention and disposition schedules. All data created or used in support of SED business operations are owned by SED, regardless of form or format.

All data both electronic and non-electronic must be assigned a classification level. The classification level should be based upon the potential impact on SED; should certain events occur which interferes with the data or systems needed to accomplish its assigned mission, responsibilities, and asset protection. Data classification must be reviewed on an ongoing basis to ensure that it has the appropriate classification level.

Please go to (Data Classification Policy) for more information regarding data classification and handling.

Associated Standards: NYS-S14-003, Information Security Controls.

VIII. Incident Response Policy

SED will respond to incidents in accordance with its Cybersecurity Incident Response Policy**.** The incident response process will determine if there is a breach. All breaches must be reported to the Chief Privacy Officer.

SED will comply with legal requirements that pertain to the notification of individuals affected by a breach or unauthorized disclosure of personally identifiable information.

Please go to (Cybersecurity Incident Response Policy) for more information regarding the incident response policy.

Associated Standards: NYSED_SECP9_V13_Cybersecurity Incident Response Policy, Cybersecurity Incident Response (CIR) Standard, and Data Privacy and Security Policy

IX. Notification

SED is subject to certain state and federal requirements that specify when an individual must be notified when there has been or is reasonably believed to have been a compromise of the individual's private information.

SED will comply with legal requirements that pertain to the notification of individuals affected by a breach or unauthorized disclosure of personally identifiable information.

State Entities must also notify non-NYS residents when there has been or is reasonably believed to have been a compromise of the individual's private information.

This policy also applies to information maintained on behalf of a State Entity by a third party.

Please go to (Breach Notification) for more information regarding the notification process.

Associated standards: Education on Law Section 2-d, State Technology Law, Article II, Internet Security and Privacy Act, and Data Privacy and Security Policy.

X. Access Control

Access to data, systems and network services must follow the Least Privileges Principles. The objective is to limit access to institutional data and IT Resources. Department must ensure that access to institutional data follows the need to know and least privileges principles. Departments/business units must ensure that institutional data is classified and has controls to prevent unauthorized access when data or systems are classified as Restricted or Confidential.

SED must route network access to institutional data classified as Restricted or Confidential through secure access control points.

SED will establish processes and procedures to ensure that Restricted and Confidential is protected and only those who have a need to know the information or to perform their duties and/or administrative functions have administrative rights to access the data can do so.

Where technically feasible, users will be provided with the minimum privileges necessary to perform their job duties.

Associated standards: NYSED Data Privacy and Security Policy.

XI. Physical Access Security

Appropriate safeguards will be implemented to limit unauthorized physical access to any Department information, computer, or computer-related device.

XII. Vulnerability Management

A vulnerability management plan for SED systems and information processing environment must be developed, documented, and implemented. Systems must be scanned for vulnerabilities. Vulnerabilities must be remediated in accordance with an assessment of risk and maximum allowable timeframes.

1. All software applications must be scanned for vulnerabilities before being installed in production and periodically thereafter.
2. All systems must have an agreed upon secure baseline configuration before being deployed in production and scanned for vulnerabilities periodically thereafter.
3. All systems and software applications are subject to periodic penetration testing.
4. Appropriate action, such as patching or updating the system, must be taken to address discovered vulnerabilities. For any discovered vulnerability, a plan of action and milestones must be created, and updated accordingly, to document the planned remedial actions to mitigate vulnerabilities.

XIII. Information Security and Privacy Training

All Users including interns, volunteers, contractors, and consultants that have access to SED data, information systems, information in electronic and non-electronic format, or data assets must complete SED's annual Information Privacy and Security Awareness training as a minimum. There may also be additional trainings required based upon job duties and access privileges.

XIV. Data Exchange Agreements

Third Party Agreements:
All agreements with third parties such as vendors, other government agencies, or contractors must include requirements to adhere to SED information security policies or other appropriate confidential security protocols. Systems that exchange data with/to any other entity must be accompanied by a signed written agreement that the entity will adhere to specific agreed upon security protocols related to the data exchange.

All vendor agreements shall contain a requirement that any SED information obtained or created as a result of such an agreement shall be the property of the SED and shall not be used, including but not limited to secondary release or disclosure, without written authorization of the SED.

5.0 Compliance

This policy shall take effect upon publication. The Information Security Office (ISO) shall review the policy at least every two years to ensure relevancy. To accomplish this assessment, ISO may issue, from time to time, requests for information to other program office departments, which will be used to develop any reporting requirements as may be requested by the Department Commissioner or designee, the Board of Regents, or Legislative entities.

Any violation of this policy may subject the user to disciplinary action, civil penalties, and/or criminal prosecution. The Department will review alleged violations of this policy on a case-by-case basis and pursue recourse, as appropriate.

6.0 Definitions of Key Terms

Breach: The unauthorized acquisition, access, use, or disclosure of student, teacher or principal PII as defined by Education law §2-d, or any SED sensitive or confidential data or a data system that stores that data, by or to a person not authorized to acquire, access, use, or receive the data.

Confidential Information: Confidential Information is information that is prohibited from disclosure by law. Access to confidential information is limited to those SED representatives who need such information to carry out their duty. When confidential information is received from another office, the receiving office must accept the responsibility for the confidential information and secure it appropriately. Examples of Confidential Information may include but are not limited to; personally identifiable information (PII) (i.e. name in combination with Social Security number (SSN) and/or financial account numbers), intellectual property (i.e. vendor or third-party copyrights, patents), passwords used for authenticating individuals, network architecture schematics

Cyber security incident: A cyber security incident is considered to be any adverse event that threatens the confidentiality, integrity or accessibility of state information resources.

Encryption: The process of encoding personal information for secure transmission across the Internet.

Information Technology (IT) Resources – A term that broadly describes IT infrastructure, software and/or hardware with computing and networking capability. These include, but are not limited to: telephones, fax machines, copiers, printers, Internet, email, and social media sites, portable computing devices and systems, mobile devices, printers, network devices, industrial control systems (SCADA, etc.), access control systems, digital video monitoring systems, data storage systems, data processing systems, backup systems, electronic media, Logical Media, biometric and access tokens and other devices that connect to any SED network. This includes both SED -owned and personally owned devices while they store Department Information, are connected to SED systems, are connected to SED Networks or used for SED business.

Media: Tools used to store and deliver information or data, including electronic (email, CD, DVD, flash drive, etc.) and paper.

Restricted Information: Restricted Information pertains to information, which is not public information, but can be disclosed to or used by SED representatives to carry out their duties, and anything that is not protected by regulation or law. Examples of Restricted Information may include but are not limited to, operational information, personnel records, information security procedures, research, or internal communications.

Software applications: is a program or group of programs designed for end users.

System: Systems include but are not limited to servers, platforms, networks, communications, databases and software applications.

10.0 ISO Contact Information

Submit all inquiries and requests for future enhancements to the policy owner at:

NEW YORK STATE EDUCATION DEPARTMENT
Information Security Office
Email: infosec@nysed.gov
Website: http://atwork.nysed.gov/iso/

11.0 Review Schedule and Revision History

Date	Description of Change	Reviewer
1/3/2002	Original Policy Released	Information Management Advisory Council
11/24/2020	Updated ISO Office and phone number, updated information in Sections 1 thru 4	Chief Information Security Officer
12/4/2020	Policy purpose, scope, and policy statements updated	ITS, CPO, CISO

12.0 Related Documents

- NYSED Breach Notification
  http://www.nysed.gov/data-privacy-security/agencies-report-data-privacysecurity-incident
- NYSED Cybersecurity Incident Response Policy
- NYSED Data Classification Policy
- NYSED Information Security Policy:
  http://atwork.nysed.gov/iso/policies/policies/NYSEDInformationSecurityPolicy.pdf

- NYSED Cybersecurity Incident Response Standard: http://atwork.nysed.gov/iso/policies/policies/NYSED_SECS1-V1_CIR.pdf

NEW YORK STATE EDUCATION DEPARTMENT Information Security Office (ISO) 89 Washington Avenue, Room 152 EB Albany, NY 12234	**NYSED ISO POLICY** Secure Disposal Standard **No: SECS6 - V:4.0: (Rev 11/25/2019)**
Issued By: NYSED Chief Information Security Officer	**Owner:** NYSED Information Security Office

1.0 Purpose and Benefits of the Standard

Department information, whether stored on Department systems, electronic media devices, printed out, or sent to or held by another organization, may contain Personal, Private, or Sensitive Information (PPSI) or Personally Identifiable Information (PII). Information systems capture, process, and store information using a wide variety of media, including paper. This information is not only located on the intended storage media but also on devices used to create, process, or transmit this information. These forms of media may require special disposal to mitigate the risk of unauthorized disclosure of information and to ensure its confidentiality.

The benefit to the department will be the secure and efficient disposal of media containing sensitive Department information.

2.0 Scope

This standard applies to all individuals, including employees, consultants, vendors, and third parties, who are responsible for disposing of PPSI/PII or responsible for the sanitization of any related electronic storage media that harbors such information.

This standard addresses the secure disposal of paper and electronic storage and associated media, provided that the disposal does not conflict with any data retention policies, laws, or regulations.

It is the responsibility of all users of Department IT resources to read and understand this standard and conduct their sanitizing and disposal in accordance with these terms. In addition, users must read and understand the NYSED Information Security Policy and its associated standards.

3.0 Information Statement

As per the NYSED Information Security Policy and NYS Information Classification Standard, information must be properly managed from its creation, through authorized use, to proper disposal.

The Department must:

- Ensure that users and custodians of information are aware of its sensitivity and the basic requirements for media sanitization and secure disposal.

- Ensure that all workforce members, including property management and custodial staff, are made aware of the media sanitation and secure disposal process to establish proper accountability for all data.
- Ensure that confidential material is destroyed only by authorized and trained personnel, whether in-house or contracted, using methods outlined in this standard.

The Department may use service providers for destruction purposes provided that the information remains secure until the destruction is completed. The service providers must follow this standard. Managers and Supervisors must ensure that maintenance or contractual agreements are in place and are sufficient in protecting the confidentiality of the system media and information commensurate with the technology or methodology specified or permitted by the Secretary of the United States department of health and human services in guidance issued under Section 13402(H)(2) of Public Law 111-5 or similar compensating control in the absence of a data classification standard.

There are many risks related to the disposal of storage media, including unauthorized release of sensitive and/or confidential information, potential violation of software agreements, and unauthorized disclosure of copyright or other intellectual property. For these reasons, the following controls must be followed.

Paper Media

All paper-based media should be properly disposed of when it is no longer necessary for business use.

- Only paper media classified as “Public” should be disposed of using the standard disposal method (i.e. these documents can be placed in a recycling bin).

The following controls apply to all paper documents unclassified, classified at a level more sensitive than public, or containing personal, private, or sensitive information (PPSI) or personally identifiable information (PII).

- Documents can be placed in a designated locked Confidential Recycling bin or shredded internally.
- Cross cut shredding, pulverizing, disintegration, or incineration are the acceptable methods of destroying documents.
- All new shredders obtained by the Department must be crosscut by shredders.
- A third-party document destruction service may be contracted for destroying quantities of paper documents.
- A “Certificate of Destruction” must be obtained from the third-party destruction service after this process.

Electronic Media

The sale, transfer, surplusage, or disposal of computers, computer peripherals, computer software, and other IT devices can create information security risks for the Department due to the storage media used in these devices.

The following controls are required for secure disposal of all electronic media.

- Prior to any sanitization process:
    - Ensure that all important data or configurations are backed up to another location.

    - Ensure that the electronic storage device is disconnected from the Department network. (This ensures only the intended device is sanitized.)
- All electronic storage devices to be disposed of must be returned to IT.

Standard Disposal

- Standard Disposal is the act of discarding media with no other sanitization considerations. This is the acceptable method to dispose of paper documents containing only public information.
- Standard Disposal is acceptable for optical media (CD's, DVD's, etc.) labeled as "Public" or with no sensitive information contained on them.
- Standard Disposal must not be used for the disposal of any Department electronic storage devices (thumb drives, USB drives, etc.). Electronic storage devices must never be placed in a garbage or recycle bin without applying additional sanitization actions.

Media Sanitization Methods—Clear, Purge, Destroy

Method	Description
Clear	One method to sanitize media is to use software or hardware products to overwrite user-addressable storage space on the media with non-sensitive data, using the standard read and write commands for the device. This process may include overwriting not only the logical storage location of a file(s) (e.g., file allocation table) but also should include all user- addressable locations. The security goal of the overwriting process is to replace Target Data with non-sensitive data. Overwriting cannot be used for media that are damaged or not rewriteable, and may not address all areas of the device where sensitive data may be retained. The media type and size may also influence whether overwriting is a suitable sanitization method. For example, flash memory-based storage devices may contain spare cells and perform wear levelling, making it infeasible for a user to sanitize all previous data using this approach because the device may not support directly addressing all areas where sensitive data has been stored using the native read and write interface. The Clear operation may vary contextually for media other than dedicated storage devices, where the device (such as a basic cell phone or a piece of office equipment) only provides the ability to return the device to factory state (typically by simply deleting the file pointers) and does not directly support the ability to rewrite or apply media-specific techniques to the non-volatile storage contents. Where rewriting is not supported, manufacturer resets and procedures that do not include rewriting might be the only option to Clear the device and associated media. These still meet the definition for Clear as long as the device interface available to the user does not facilitate retrieval of the Cleared
Purge	Some methods of purging (which vary by media and must be applied with considerations described further throughout this document) include overwrite, block erase, and Cryptographic Erase, through the use of dedicated, standardized device sanitize commands that apply media-specific techniques to bypass the abstraction inherent in typical read and write commands. Destructive techniques also render the device Purged when effectively applied to the appropriate media type, including incineration, shredding, disintegrating, degaussing, and pulverizing. The common benefit across all these approaches is assurance that the data is infeasible to recover using state of the art laboratory techniques. However, Bending, Cutting, and the use of some emergency procedures (such as using a firearm to shoot a hole through a storage device) may only damage the media as portions of the media may remain undamaged and therefore accessible using advanced laboratory techniques. Degaussing renders a Legacy Magnetic Device Purged when the strength of the degausser is carefully matched to the media coercivity. Coercivity may be difficult to determine based only on information provided on the label. Therefore, refer to the device

	flash memory-based storage devices or for magnetic storage devices that also contain non-volatile non-magnetic storage. Degaussing renders many types of devices unusable (and in those cases, Degaussing is also a Destruction technique).
Destroy	There are many different types, techniques, and procedures for media Destruction. While some techniques may render the Target Data infeasible to retrieve through the device interface and unable to be used for subsequent storage of data, the device is not considered Destroyed unless Target Data retrieval is infeasible using state of the art laboratory techniques. *Disintegrate, Pulverize, Melt, and Incinerate.* These sanitization methods are designed to completely Destroy the media. They are typically carried out at an outsourced metal Destruction or licensed incineration facility with the specific capabilities to perform these activities effectively, securely, and safely. *Shred*. Paper shredders can be used to Destroy flexible media such as diskettes once the media are physically removed from their outer containers. The shred size of the refuse should be small enough that there is reasonable assurance in proportion to the data confidentiality that the data cannot be reconstructed. To make reconstructing the data even more difficult, the shredded material can be mixed with non-sensitive material of the same type (e.g., shredded paper or shredded flexible media). The application of Destructive techniques may be the only option when the media fails and other Clear or Purge techniques cannot be effectively applied to the media, or when the

Table 5-1: Sanitization Methods
(from NIST 800-88, Rev. 1, Guidelines for Media Sanitization)

Sanitization Decision Process

The decision process is based on the confidentiality of the information, not the type of media. The Department chooses the type of sanitization to be used, and the type of sanitization is approved by the Information Owner and Information Steward. The technology used may vary by media type and by the technology available to the custodian, so long as the requirements of the sanitization type are met.

Disposal without sanitization should be considered only if information disclosure would have no impact on organizational mission, would not result in damage to organizational assets, and would not result in financial loss or harm to any individuals.

The security categorization of the information, along with internal environmental factors, should drive the decisions on how to deal with the media. The key is to first think in terms of information confidentiality, then apply considerations based on media type.

The cost versus benefit of a sanitization process should be understood prior to a final decision. The Department can always increase the level of sanitization applied if that is reasonable and indicated by an assessment of the existing risk. For example, even though Clear or Purge may be the recommended solution, it may be more cost-effective (considering training, tracking, and validation, etc.) to destroy media rather than use one of the other options. The Department may not decrease the level of sanitization required.

Electronic Storage Device Destruction Process

If electronic storage devices are destroyed within the Department, the following requirements must be met:

- All electronic storage devices to be destroyed must be returned to IT for destruction.
- Hard drives returned to IT for destruction must be destroyed as soon as they are received by IT.
- If hard drives are not destroyed immediately, they must be labeled that they need destruction, and stored in a secure locked location.

- After hard drives have been destroyed they must be sent to a third-party destruction service for final drive shredding and recycling.
- IT must maintain a record of the destruction to document what media were destroyed, when, how they were destroyed, and the final disposition of the media.

Documenting the Secure Disposal of Media and Devices

- The disposal of media and electronic storage devices containing PPSI or PII shall be documented.
- No storage device may be sent to surplus, recycled, returned to manufacturer, or leave the Department for any other reason without either being sanitized or destroyed, and with the appropriate documentation completed. For example:
    - Desktop systems returned to manufacturers due to contracts need to have the hard drives sanitized prior to sending back to the manufacturer.
    - Servers cannot leave the Department with their hard drives. Server hard drives must be destroyed, and the process documented.
- The documentation must include the name of the person authorizing the disposal and the reason for disposal.
- The documentation must include the disposal method and include the date the disposal took place and a log of the device being disposed containing these items.

Disposal of Sanitized Equipment

- Once sanitized, electronic equipment must be disposed of or sent to surplus in an environmentally sound manner. This includes all hardware, including servers, desktops, laptops, network equipment, destroyed disks, external, and removable storage, etc.
- Electronic equipment being disposed of should never be put in a trash bin or dumpster.

Privacy Breach Reporting

- The Information Security Office (ISO) will review compliance to this standard and will report any misuse or improper disposal of PPSI or PII to the Chief Privacy Officer (CPO). In accordance with the Data Privacy and Security Policy and regulations (e.g. NYS Technology Law, the NYS Personal Privacy Protection Law, among others), the ISO and CPO may also be required to notify the state attorney general, the consumer protection board, and the state office of cyber security and critical infrastructure coordination.

4.0 Compliance

This standard shall take effect upon publication. The Information Security Office (ISO) shall review the standard at least every two years to ensure relevancy. To accomplish this assessment, the ISO may issue requests for information from other program office departments. The information garnered will be used to develop any reporting requirements as may be requested by the Department Chief Privacy Officer, the Board of Regents, or Legislative entities.

Any violation of this standard may subject the user to disciplinary action up to and including termination. The Department will review alleged violations of this standard on a case-by-case basis and pursue recourse, as appropriate.

5.0 Definitions of Key Terms

Electronic Storage Device: Any electronic device that can be used to store data. This includes but is not limited to internal and external hard drives, USB drives, SD cards, etc.

Electronic Media: Any material on which electronic data may be stored, such as magnetic tape, magnetic disks, solid state storage devices, or optical discs.

Solid-State Storage Device: A type of computer storage media that is made from microchips. Solid-state media stores data electronically instead of magnetically, as spinning hard disk drives, or magnetic oxide tape do. Examples include thumb drives, memory sticks, SD cards, Solid-State Disks (SSD), etc.

Standard Disposal: The act of discarding media with no other sanitization considerations. Simply discarding the media. An example would be by placing paper documents in a recycling bin.

Clearing: A level of sanitization that renders media unreadable through normal means. Simple deletion of items would not suffice for clearing. Clearing is typically accomplished through an overwriting process that replaces actual data with 0's or random characters. Overwriting cannot be used for media that is damaged or not writeable.

Purging: Purging is the removal of data from a system or storage device with the intent that the data cannot be reconstructed by any known technique. Purging typically consist of using specialized utilities that repeated overwrite data.

Destroying: Rendering media unusable. After media is destroyed, it cannot be reused as originally intended. Physical destruction can be accomplished using a variety of methods, including crushing, disintegration, incineration, pulverizing, shredding, and melting. Optical storage media, including CD, CD-RW, CD_R, CD-ROM, DVD, Blu-ray, and magneto-optic (MO) disks are typically destroyed.

6.0 ISO Contact Information

Submit all inquiries and requests for future enhancements to the standard owner at:

NEW YORK STATE EDUCATION DEPARTMENT
Information Security Office
Website: http://atwork.nysed.gov/iso/
Email: infosec@nysed.gov

7.0 Review Schedule and Revision History

Date	Description of Change	Reviewer
08/03/2017	DRAFT	CISO
3/12/2019	Updated ISO Office and phone number, updated information in Section 1, and 4	Marlowe Cochran, Chief Information Security Officer
8/9/2019	Reviewed, Update standard terms	ITS, CPO, CISO
11/25/2019	Updated Contact Information	Marlowe Cochran, Chief Information Security Officer
12/5/2019	Original Standard Release	Marlowe Cochran, Chief Information Security Officer

8.0 Related Documents

- NYSED Information Security Policy
- NIST 800-88, Rev. 1, Guidelines for Media Sanitization
- Data Privacy and Security Policy
- NYS Information Classification Standard

NEW YORK STATE EDUCATION DEPARTMENT Information Security Office (ISO) 89 Washington Avenue Albany, NY 12234	**NYSED ISO STANDARD** Secure Remote Access Standard **SECS5 – V:4.0 (REV 11/25/19)**
Issued By: NYSED Chief Information Security Officer	**Owner:** NYSED Information Security Office

1.0 Purpose and Benefits of the Standard

The purpose of this standard is to effectively document, manage, and control remote access to the NYSED (the Department) computer network, and to define the protection and security requirements that support remote access. It is necessary for the Department to ensure network security by limiting the risk of intrusion and/or unauthorized access.

The benefit to the Department will be an enhanced security of Departmental information through secure and proper use of all remote access resources.

2.0 Scope

This standard applies to all Department IT remote access resources and all users of such resources.

It is the responsibility of users to read and understand this standard and to conduct their activities in accordance with its terms. In addition, users must read and understand the NYSED Information Security Standard and its associated standards.

3.0 Information Statement

General Requirements

Remote access to the Department's network is subject to the following requirements:

- Remote access must be for Department business purposes only. Access will be limited to those resources and levels required for relevant business functions.
- Remote access to the Department's network is limited to within the United States. Any access required outside of the United States will require further approval by the Information Security Office.
- Remote users only have access to resources within the Department's network that they require.
- Remote access activity will be logged and monitored for suspicious activity.
- Remote access sessions must not last any longer than 24 hours.
- All changes to the configuration of infrastructure equipment that supports remote access must follow the applicable Department change management processes. If a formal change management process

doesn't exist, all changes to the configuration of infrastructure equipment that supports remote access must be well documented and securely stored.

- All remote access connections (e.g. circuits with Virtual Private Network (VPN) tunnels to other facilities) or connection types (e.g. laptops using VPNs) must be approved by the Information Security Office (ISO), via the Secure Remote Access Request Form.
- All users that receives remote access will be required to take a remote access training; this training will be an annual requirement for those who need to maintain their privileged access to work remotely.

Virtual Private Network (VPN)

The remote access capabilities of all Department employees, contractors, and vendors are subject to the same security protections, policies, standards, and procedures as on-site connections. All Department information security policies, including the NYSED Acceptable Use of IT Resources policy, are applicable to the remote access environment. The following controls are required for all VPN connections:

- Remote access permissions must be associated with a single remote user and/or system.
- Remote access authorization must not be transferred to or used by another person.
- Authorized requests for non-Department employees (vendors, contractors, consultants, etc.) for VPN privileges must be requested by the business unit manager who requires the Department non-employee to have access. This request must be based on a business need. Approval by the Director of Operations (or the Deputy Commissioner), and the Information Security Office (ISO) is required. Further, an Information Protection Agreement (IPA) will need to be completed.
- VPN access requires strong authentication. See the Department User Account Password Policy for details.
- Users with remote access will receive required software and instructions for use from the desktop support team.
- Remote connections for contractors and other temporary employees using approved non-Department issued devices must be implemented using either Secure Sockets Layer (SSL) VPN portal connection or through a Citrix solution such as XenDesktop or XenApp.
- Department-issued laptops, computers, or workstations that connect remotely must have up-to-date anti-virus signatures and properly patched and updated versions of the operating systems and programs.
- VPN client connections must have an idle timeout.

Direct External Vendor Access

The following controls must be followed in situations where access to an external vendor's application requires non-Department equipment to be connected to the Department's network. For example, access to other financial institution's applications or file transfers may require direct access from the vendor's networks to the Department's network.

- The external vendor will be required to limit outbound traffic (into the NYSED network) to only the clients and services necessary to support the target application. The Department must not allow a

wide range of the vendor's Internet addresses to access the Department's network; only the required addresses will be allowed.

- All external vendor circuits and equipment will terminate on a common network segment, which will be segregated from the rest of the network by a firewall.
- Firewall rules will limit traffic to that which is required for the target application.
- Firewall rules will be applied on both incoming and outgoing network traffic to ensure security of the network and to ensure that external vendors are properly limiting access through their equipment.

Remote Support Sessions

Remote support sessions may be required for vendors or other support persons to remotely connect to a Department system to resolve a problem. A remote support session (e.g. GoToMeeting, Cisco WebEx, etc.) may include screen sharing and/or remote control. The following security controls are required when a remote session is needed:

- Any remote session requiring direct access to a Department IT resource (e.g. a personal computer (PC) or server) must be approved by the Information Security Office.
- All remote support sessions must be conducted through an SSL/TSL or other encrypted connection.
- When a vendor requires a remote support session, a session log must be enabled for the whole session.
- While a remote support session is in progress, all activity must be physically monitored by a Department employee to ensure that no inappropriate access or activities take place.
- Any window or file that is not involved in the remote support session must be closed prior to allowing remote access to the system.

4.0 Compliance

This standard shall take effect upon publication. The Information Security Office (ISO) shall review the standard at least every two years to ensure relevancy. To accomplish this assessment, the ISO may issue, from time to time, requests for information to other office departments, which will be used to develop any reporting requirements as may be requested by the Department Chief Privacy Officer, the Board of Regents, or Legislative entities.

If compliance with this standard is not feasible or technically possible, or if deviation from this standard is necessary to support a business function, the office shall request an exception through the NYSED Information Security Exception Standard process.

Any violation of this standard may subject the user to disciplinary action up to and including termination. The Department will review alleged violations of this standard on a case-by-case basis and pursue recourse, as appropriate.

5.0 Definitions of Key Terms

Information Technology (IT) Resources: Equipment or services used to input, store, process, transmit, and output information, including, but not limited to, desktops, laptops, mobile devices, servers, telephones, fax machines, copiers, printers, Internet, email, and social media sites.

Virtual Private Network (VPN): A secure private network that uses the public communications infrastructure to transmit data.

6.0 ISO Contact Information

Submit all inquiries and requests for future enhancements to the standard owner at:

NEW YORK STATE EDUCATION DEPARTMENT
Information Security Office
Website: http://atwork.nysed.gov/iso/
Email: infosec@nysed.gov

7.0 Review Schedule and Revision History

Date	Description of Change	Reviewer
8/10/2017	Draft	CISO
3/12/2019	Updated ISO Office and phone number, updated information in Section 1, and 4	Marlowe Cochran, Chief Information Security Officer
7/8/2019	Reviewed, Removed remote session timeout	ITS, CPO, CISO
11/25/2019	Updated Contact Information	Marlowe Cochran, Chief Information Security Officer
12/5/2019	Original Standard Release	Marlowe Cochran, Chief Information Security Officer

8.0 Related Documents

- NYSED Information Security Standard
- NYSED Acceptable Use of Information Technology (IT) Resources Standard
- NYSED User Account Password Policy
- NYSED Information Protection Agreement Procedure

NEW YORK STATE EDUCATION DEPARTMENT Information Security Office (ISO) 89 Washington Avenue Albany, NY 12234	**NYSED ISO POLICY** Service Account Password Policy **No: SECP8 - V:4.0: (REV 2/18/2020)**
Issued By: NYSED Chief Information Security Officer	**Owner:** NYSED Information Security Office

1.0 Purpose and Benefits of the Policy

Passwords are an important part of the Department's information security program. Strong passwords applied to Department Information Technology (IT) resources reduce the risk of unauthorized access to electronic information. The purpose of this policy is to establish a standard for the creation of strong passwords, the protection of those passwords, and the frequency of changing these passwords.

The benefit to the Department will be an enhanced security of Departmental information through use of stronger passwords.

2.0 Scope

There are four types of logon accounts used by the Department:

1. User Accounts – Unique accounts issued to a single Individual (i.e. employees, vendors, consultants, interns, volunteers, affiliates, etc.), often referred to as 'end-users' and do not possess the privileges as an administrative account.

2. Administrative Accounts (Privileged) – Unique accounts issued to a single Individual, but these accounts have a higher degree of access privileges to systems (e.g. 'root' access on a Unix system). These accounts are intended to be used by authorized personnel only (such as IT personnel), for performing administrative tasks such as maintaining user accounts, performing password resets, and managing systems.

3. Public/Anonymous accounts – Use of these accounts is purposefully unrestricted. There may or may not be an associated password with such accounts, but when there is such a password, the password may be shared freely (e.g. public wireless password provided in a conference room). In such cases, as a matter of best practice and as feasible, the public password shall follow strong password rules as described for user and administrative account password requirements, below.

4. Service Accounts – Used only for automated processes between systems. These accounts are not to be used by individuals to login to systems, with the exception of troubleshooting to ensure that the account is working properly.

This policy applies to all Service Accounts.

User, Administrative, and to Public/Anonymous accounts are covered under the NYSED User Account Password Policy (SECP5).

It is the responsibility of all users of Department IT resources to read and understand this policy and to create their passwords in accordance with its terms. In addition, users must read and understand the NYSED Information Security Policy and its associated policies and standards.

3.0 General Password Requirements

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of the Department's entire network. As such, all users and administrators are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords. It is important to set a strong password and change them regularly.

The following password minimum requirements apply to ALL logon accounts:

- Passwords:
  - Must never be shared or displayed on a screen.
  - Must be classified and handled as Department Confidential information.
  - Must be changed whenever there is any indication of compromise.
  - Must not be reused for at least 4 iterations.
  - Must be encrypted when transmitted electronically with a strong encryption protocol
  - Must be encrypted or hashed when held in storage.
  - When embedded in configuration files, source code or scripts, they must be either encrypted or secured with compensating controls which provide a comparable level of protection.
- Whenever technically feasible, a password-protected screen lock must be activated on a system after 10 minutes of user inactivity.
- Whenever technically feasible, all systems that provide access to sensitive, restricted, or confidential information must automatically disable an account after six (6) sequential invalid login attempts within a fifteen (15) minute period. After such account is disabled, the account must remain disabled for a minimum of fifteen (15) minutes.
- Department system passwords should be different than any other non-Department system passwords used by an individual (e.g. a social media site password such as for Facebook should not be the same as the one used by an individual to login to the NYSED network).

4.0 Service Account Password Requirements

For service accounts, a password is used to authenticate or identify a service or a system. Service accounts are created by System Administrators and are often shared within a group.

The System Administrator and/or group is responsible for selecting and protecting passwords that provide security for the Department information that is accessible by the service or system. The following password minimum requirements must be met:

- Any system administrator or group that suspects that a password has been compromised must report this information security incident to the Information Security Office immediately (infosec@nysed.gov).
- Systems are often initially installed with default passwords. Default passwords must be changed immediately upon the completion of the installation process and/or first login.

- Service account passwords must only be known to system administrators and groups on a ‘need-to-know’ basis. The names of such service accounts and the names of system administrators that have access to them must be documented. These lists must be kept current.
- Service account management may be enhanced by the use of an on-premise password management software (e.g. Password Safe, KeePass, Secret Server), but such software must be approved by the Information Security Office (ISO).
- When a system administrator leaves the Department, or changes their job function within the Department, the service account passwords that they had access to must be reset.
- Service accounts require a strong/complex password, regardless of whether an IT resource allows for a weaker password.
    - Passwords must be a minimum of 8 characters (15 characters or more is recommended).
    - Whenever technically feasible by the IT resource, passwords must contain at least three of the four requirements below:
        - An uppercase character.
        - A lowercase character.
        - A numeric character.
        - A special character. For example: #$&*
            - NOTE: some systems do not allow use of certain special characters
    - Some legacy systems may not have the capability to enforce these rules, in those cases it is up to the individual to select a password that meets these requirements.
- Whenever technically feasible, service accounts should be restricted to logons from specific IP addresses.
- Service account passwords must also:
    - Never be written down and/or posted in a work area.
    - Never be sent electronically unencrypted (e.g. through unencrypted email).
    - Never be recorded in a non-encrypted stored document.
    - Never be shared with anyone that is not authorized on a ‘need-to-know’ basis.
    - Never have hints shared with anyone concerning the format of these passwords.
    - Never be used with the "Remember Password" feature of application programs such as Internet Explorer, email systems, or any other program.
    - Never be revealed by letting someone look over your shoulder when typing the password.
- Each system administrator is directly responsible for use of service account passwords. Any action or activity taken with a password will be attributed to the system administrator or group that owns the password.

5.0 Technical Access Controls

Wherever technically feasible, technical access controls will be enabled on Department IT resources to ensure that the password minimum requirements stated above are enforced (e.g. Microsoft Active Directory Password Complexity rules will be enabled). Wherever not technically feasible, equivalent controls must be established through other methods or procedures. For instance, a system administrator can use software tools periodically to detect weak passwords and require users with such to change them.

Department IT resources may also incorporate multi-factor authentication access controls in order to enhance the security of highly sensitive Department information.

6.0 Password Reset Assistance

System Administrators have the authority and ability to reset system passwords where proper authorization has been given and audit trails are in place.

7.0 Compliance

This policy shall take effect upon publication. The Information Security Office (ISO) shall review the policy at least every two years to ensure relevancy. To accomplish this assessment, ISO may issue requests for information from other program office departments. The information garnered will be used to develop any reporting requirements as may be requested by the Department Chief Privacy Officer, the Board of Regents, or Legislative entities.

Compliance with this policy is the responsibility of all administrators of Department service accounts. All such individuals have the responsibility to protect service account passwords and the information that may be accessed by such accounts if the password were to be compromised.

If compliance with this policy is not feasible or technically possible, or if deviation from this policy is necessary to support a business function; the office shall request an exception through the NYSED Information Security Exception Policy process.

Any violation of this standard may subject the user to disciplinary action up to and including termination. The Department will review alleged violations of this policy on a case-by-case basis and pursue recourse, as appropriate.

8.0 Definitions of Key Terms

Information Technology (IT) Resources – Equipment or services used to input, store, process, transmit, and output information, including, but not limited to, desktops, laptops, mobile devices, servers, telephones, fax machines, copiers, printers, Internet, email, and social media sites.

Multi-factor Authentication – a method of computer access control in which a user is only granted access after successfully presenting several separate pieces of evidence to an authentication mechanism – typically at least two of the following categories: knowledge (something they know), possession (something they have), and inherence (something they are) (Rosenblatt & Cipriani, 2013).

9.0 ISO Contact Information

Submit all inquiries and requests for future enhancements to the policy owner at:

NEW YORK STATE EDUCATION DEPARTMENT
Information Security Office
Website: http://atwork.nysed.gov/iso/
Email: infosec@nysed.gov

10.0 Review Schedule and Revision History

Date	Description of Change	Reviewer
08/03/2017	DRAFT	CISO
3/12/2019	Updated ISO Office and phone number, updated information in Section 1, 3 and 7	Marlowe Cochran, Chief Information Security Officer
11/25/2019	Reviewed, Updated Contact Information	ITS, CPO, CISO
12/5/2019	Original Standard Release	Marlowe Cochran, Chief Information Security Officer
2/18/20	Updated the language in the Compliance section	Marlowe Cochran, Chief Information Security Officer

11.0 Related Documents

- NYSED Information Security Policy
- NYSED Information Security Exception Policy
- NYSED User Account Password Policy

12.0 References

1. Rosenblatt, S., & Cipriani, J. (2013). Two-factor authentication: What you need to know (FAQ). Retrieved December 06, 2016, from https://www.cnet.com/news/two-factor-authentication-what-you-need-to-know-faq/