Attachment S
PARENTS' BILL OF RIGHTS
FOR DATA PRIVACY AND SECURITY

To satisfy their responsibilities regarding the provision of education to students in pre-kindergarten through grade twelve, "educational agencies" (as defined below) in the State of New York collect and maintain certain personally identifiable information from the education records of their students. As part of the Common Core Implementation Reform Act, Education Law §2-d requires that each educational agency in the State of New York must develop a Parents' Bill of Rights for Data Privacy and Security (Parents' Bill of Rights). The Parents' Bill of Rights must be published on the website of each educational agency, and must be included with every contract the educational agency enters into with a "third party contractor" (as defined below) where the third party contractor receives student data, or certain protected teacher/principal data related to Annual Professional Performance Reviews that is designated as confidential pursuant to Education Law §3012-c ("APPR data").

The purpose of the Parents' Bill of Rights is to inform parents (which also include legal guardians or persons in parental relation to a student, but generally not the parents of a student who is age eighteen or over) of the legal requirements regarding privacy, security and use of student data. In addition to the federal Family Educational Rights and Privacy Act (FERPA), Education Law §2-d provides important new protections for student data, and new remedies for breaches of the responsibility to maintain the security and confidentiality of such data.

A. <u>What are the essential parents' rights under the Family Educational Rights and Privacy Act (FERPA) relating to personally identifiable information in their child's student records?</u>

The rights of parents under FERPA are summarized in the Model Notification of Rights prepared by the United States Department of Education for use by schools in providing annual notification of rights to parents. It can be accessed at http://www2.ed.gov/policy/gen/guid/fpco/ferpa/lea-officials.html, and a copy is attached to this Parents' Bill of Rights. Complete student records are maintained by schools and school districts, and not at the New York State Education Department (NYSED). Further, NYSED would need to establish and implement a means to verify a parent's identity and right of access to records before processing a request for records to the school or school district. Therefore, requests to access student records will be most efficiently managed at the school or school district level.

Parents' rights under FERPA include:

1. The right to inspect and review the student's education records within 45 days after the day the school or school district receives a request for access.

2. The right to request amendment of the student's education records that the parent or eligible student believes are inaccurate, misleading, or otherwise in violation of the student's privacy rights under FERPA. Complete student records are maintained by schools and school districts and not at NYSED, which is the secondary repository of data, and NYSED make amendments to school or school district records. Schools and school districts are in the best position to make corrections to students' education records.

3. The right to provide written consent before the school discloses personally identifiable information (PII) from the student's education records, except to the extent that FERPA authorizes disclosure without consent (including but not limited to disclosure under specified conditions to: (i) school

officials within the school or school district with legitimate educational interests; (ii) officials of another school for purposes of enrollment or transfer; (iii) third party contractors providing services to, or performing functions for an educational agency; (iv) authorized representatives of the U. S. Comptroller General, the U. S. Attorney General, the U.S. Secretary of Education, or State and local educational authorities, such as NYSED; (iv) (v) organizations conducting studies for or on behalf of educational agencies) and (vi) the public where the school or school district has designated certain student data as "directory information" (described below). The attached FERPA Model Notification of Rights more fully describes the exceptions to the consent requirement under FERPA).

4. Where a school or school district has a policy of releasing "directory information" from student records, the parent has a right to refuse to let the school or school district designate any all of such information as directory information. Directory information, as defined in federal regulations, includes: the student's name, address, telephone number, email address, photograph, date and place of birth, major field of study, grade level, enrollment status, dates of attendance, participation in officially recognized activities and sports, weight and height of members of athletic teams, degrees, honors and awards received and the most recent educational agency or institution attended. Where disclosure without consent is otherwise authorized under FERPA, however, a parent's refusal to permit disclosure of directory information does not prevent disclosure pursuant to such separate authorization.

5. The right to file a complaint with the U.S. Department of Education concerning alleged failures by the School to comply with the requirements of FERPA.

B. What are parents' rights under the Personal Privacy Protection Law (PPPL), Article 6-A of the Public Officers Law relating to records held by State agencies?

The PPPL (Public Officers Law §§91-99) applies to all records of State agencies and is not specific to student records or to parents. It does not apply to school districts or other local educational agencies. It imposes duties on State agencies to have procedures in place to protect from disclosure of "personal information," defined as information which because of a name, number, symbol, mark or other identifier, can be used to identify a "data subject" (in this case the student or the student's parent). Like FERPA, the PPPL confers a right on the data subject (student or the student's parent) to access to State agency records relating to them and requires State agencies to have procedures for correction or amendment of records.

A more detailed description of the PPPL is available from the Committee on Open Government of the New York Department of State. Guidance on what you should know about the PPPL can be accessed at http://www.dos.ny.gov/coog/shldno1.html. The Committee on Open Government's address is Committee on Open Government, Department of State, One Commerce Plaza, 99 Washington Avenue, suite 650, Albany, NY 12231, their email address is coog@dos.ny.gov, and their telephone number is (518) 474-2518.

C. Parents' Rights Under Education Law §2-d relating to Unauthorized Release of Personally Identifiable Information

1. What "educational agencies" are included in the requirements of Education Law §2-d?

- The New York State Education Department ("NYSED");
- Each public school district;
- Each Board of Cooperative Educational Services or BOCES; and
- All schools that are:
  - a public elementary or secondary school;

- a universal pre-kindergarten program authorized pursuant to Education Law §3602-e;
- an approved provider of preschool special education services;
- any other publicly funded pre-kindergarten program;
- a school serving children in a special act school district as defined in Education Law 4001; or
- certain schools for the education of students with disabilities - an approved private school, a state-supported school subject to the provisions of Education Law Article 85, or a state-operated school subject to Education Law Article 87 or 88.

2. What kind of student data is subject to the confidentiality and security requirements of Education Law §2-d?

The law applies to personally identifiable information contained in student records of an educational agency listed above. The term "student" refers to any person attending or seeking to enroll in an educational agency, and the term "personally identifiable information" ("PII") uses the definition provided in FERPA. Under FERPA, personally identifiable information or PII includes, but is not limited to:

(a) The student's name;
(b) The name of the student's parent or other family members;
(c) The address of the student or student's family;
(d) A personal identifier, such as the student's social security number, student number, or biometric record;
(e) Other indirect identifiers, such as the student's date of birth, place of birth, and Mother's Maiden Name[1];
(f) Other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty; or
(g) Information requested by a person who the educational agency or institution reasonably believes knows the identity of the student to whom the education record relates.

3. What kind of student data is *not* subject to the confidentiality and security requirements of Education Law §2-d?

The confidentiality and privacy provisions of Education Law §2-d and FERPA extend only to PII, and not to student data that is not personally identifiable. Therefore, de-identified data (e.g., data regarding students that uses random identifiers), aggregated data (e.g., data reported at the school district level) or anonymized data that could not be used to identify a particular student is not considered to be PII and is not within the purview of Education Law §2-d or within the scope of this Parents' Bill of Rights.

4. What are my rights under Education Law § 2-d as a parent regarding my student's PII?

Education Law §2-d ensures that, in addition to all of the protections and rights of parents under the federal FERPA law, certain rights will also be provided under the Education Law. These rights include, but are not limited to, the following elements:

(A) A student's PII cannot be sold or released by the educational agency for any commercial or marketing purposes.

[1] Please note that NYSED does not collect certain information defined in FERPA, such as students' social security numbers, biometric records, mother's maiden name (unless used as the mother's legal name).

- PII may be used for purposes of a contract that provides payment to a vendor for providing services to an educational agency as permitted by law.
- However, sale of PII to a third party solely for commercial purposes or receipt of payment by an educational agency, or disclosure of PII that is not related to a service being provided to the educational agency, is strictly prohibited.

(B) Parents have the right to inspect and review the complete contents of their child's education record including any student data stored or maintained by an educational agency.

- This right of inspection is consistent with the requirements of FERPA. In addition to the right of inspection of the educational record, Education Law §2-d provides a specific right for parents to inspect or receive copies of any data in the student's educational record.
- NYSED will develop policies for annual notification by educational agencies to parents regarding the right to request student data. Such policies will specify a reasonable time for the educational agency to comply with such requests.
- The policies will also require security measures when providing student data to parents, to ensure that only authorized individuals receive such data. A parent may be asked for information or verifications reasonably necessary to ensure that he or she is in fact the student's parent and is authorized to receive such information pursuant to law.

(C) State and federal laws protect the confidentiality of PII, and safeguards associated with industry standards and best practices, including, but not limited to, encryption, firewalls, and password protection, must be in place when data is stored or transferred.

Education Law §2-d also specifically provides certain limitations on the collection of data by educational agencies, including, but not limited to:

(A) A mandate that, except as otherwise specifically authorized by law, NYSED shall only collect PII relating to an educational purpose;

(B) NYSED may only require districts to submit PII, including data on disability status and student suspensions, where such release is required by law or otherwise authorized under FERPA and/or the New York State Personal Privacy Law; and

(C) Except as required by law or in the case of educational enrollment data, school districts shall not report to NYSED student data regarding juvenile delinquency records, criminal records, medical and health records or student biometric information.

(D) Parents may access the NYSED Student Data Elements List, a complete list of all student data elements collected by NYSED, at http://www.p12.nysed.gov/irs/sirs/documentation/NYSEDstudentData.xlsx, or may obtain a copy of this list by writing to the Office of Information & Reporting Services, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, NY 12234; and

(E) Parents have the right to file complaints with an educational agency about possible breaches of student data by that educational agency's third party contractors or their employees, officers, or assignees, or with NYSED. Complaints to NYSED should be directed in writing to the Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany NY 12234, email to CPO@nysed.gov. The complaint process is under development and will be

established through regulations to be proposed by NYSED's Chief Privacy Officer, who has not yet been appointed.

- Specifically, the Commissioner of Education, after consultation with the Chief Privacy Officer, will promulgate regulations establishing procedures for the submission of complaints from parents, classroom teachers or building principals, or other staff of an educational agency, making allegations of improper disclosure of student data and/or teacher or principal APPR data by a third party contractor or its officers, employees or assignees.

- When appointed, the Chief Privacy Officer of NYSED will also provide a procedure within NYSED whereby parents, students, teachers, superintendents, school board members, principals, and other persons or entities may request information pertaining to student data or teacher or principal APPR data in a timely and efficient manner.

5. Must additional elements be included in the Parents' Bill of Rights.?

Yes**.** For purposes of further ensuring confidentiality and security of student data, as an appendix to the Parents' Bill of Rights each contract an educational agency enters into with a third party contractor shall include the following supplemental information:

(A) the exclusive purposes for which the student data, or teacher or principal data, will be used;

(B) how the third party contractor will ensure that the subcontractors, persons or entities that the third party contractor will share the student data or teacher or principal data with, if any, will abide by data protection and security requirements;

(C) when the agreement with the third party contractor expires and what happens to the student data or teacher or principal data upon expiration of the agreement;

(D) if and how a parent, student, eligible student, teacher or principal may challenge the accuracy of the student data or teacher or principal data that is collected; and

(E) where the student data or teacher or principal data will be stored (described in such a manner as to protect data security), and the security protections taken to ensure such data will be protected, including whether such data will be encrypted.

a. In addition, the Chief Privacy Officer, with input from parents and other education and expert stakeholders, is required to develop additional elements of the Parents' Bill of Rights to be prescribed in Regulations of the Commissioner.

6. What protections are required to be in place if an educational agency contracts with a third party contractor to provide services, and the contract requires the disclosure of PII to the third party contractor?

Education Law §2-d provides very specific protections for contracts with "third party contractors", defined as any person or entity, other than an educational agency, that receives student data or teacher or principal data from an educational agency pursuant to a contract or other written agreement for purposes of providing services to such educational agency. The term "third party contractor" also includes an educational partnership organization that receives student and/or teacher or principal APPR data from a school district to carry out its responsibilities pursuant to Education Law §211-e, and a not-for-profit corporation or other non-profit organization, which are not themselves covered by the definition of an "educational agency."

Services of a third party contractor covered under Education Law §2-d include, but not limited to, data management or storage services, conducting studies for or on behalf of the educational agency, or audit or evaluation of publicly funded programs.

When an educational agency enters into a contract with a third party contractor, under which the third party contractor will receive student data, the contract or agreement must include a data security and privacy plan that outlines how all state, federal, and local data security and privacy contract requirements will be implemented over the life of the contract, consistent with the educational agency's policy on data security and privacy. However, the standards for an educational agency's policy on data security and privacy must be prescribed in Regulations of the Commissioner that have not yet been promulgated. A signed copy of the Parents' Bill of Rights must be included, as well as a requirement that any officers or employees of the third party contractor and its assignees who have access to student data or teacher or principal data have received or will receive training on the federal and state law governing confidentiality of such data prior to receiving access.

Each third party contractor that enters into a contract or other written agreement with an educational agency under which the third party contractor will receive student data or teacher or principal data shall:

- limit internal access to education records to those individuals that are determined to have legitimate educational interests
- not use the education records for any other purposes than those explicitly authorized in its contract;
- except for authorized representatives of the third party contractor to the extent they are carrying out the contract, not disclose any PII to any other party (i) without the prior written consent of the parent or eligible student; or (ii) unless required by statute or court order and the party provides a notice of the disclosure to NYSED, district board of education, or institution that provided the information no later than the time the information is disclosed, unless providing notice of the disclosure is expressly prohibited by the statute or court order;
- maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of PII in its custody; and
- use encryption technology to protect data while in motion or in its custody from unauthorized disclosure.

7. What steps can and must be taken in the event of a breach of confidentiality or security?

Upon receipt of a complaint or other information indicating that a third party contractor may have improperly disclosed student data, or teacher or principal APPR data, NYSED's Chief Privacy Officer is authorized to investigate, visit, examine and inspect the third party contractor's facilities and records and obtain documentation from, or require the testimony of, any party relating to the alleged improper disclosure of student data or teacher or principal APPR data.

Where there is a breach and unauthorized release of PII by a by a third party contractor or its assignees (e.g., a subcontractor): (i) the third party contractor must notify the educational agency of the breach in the most expedient way possible and without unreasonable delay; (ii) the educational agency must notify the parent in the most expedient way possible and without unreasonable delay; and (iii) the third party contractor may be subject to certain penalties including, but not limited to, a monetary fine; mandatory training regarding federal and state law governing the confidentiality of student data, or teacher or principal APPR data; and preclusion

from accessing any student data, or teacher or principal APPR data, from an educational agency for a fixed period up to five years.

8. Data Security and Privacy Standards

Upon appointment, NYSED's Chief Privacy Officer will be required to develop, with input from experts, standards for educational agency data security and privacy policies. The Commissioner will then promulgate regulations implementing these data security and privacy standards.

9. No Private Right of Action

Please note that Education Law §2-d explicitly states that it does not create a private right of action against NYSED or any other educational agency, such as a school, school district or BOCES.

ATTACHMENT

Model Notification of Rights under FERPA for Elementary and Secondary Schools

The Family Educational Rights and Privacy Act (FERPA) affords parents and students who are 18 years of age or older ("eligible students") certain rights with respect to the student's education records. These rights are:

1. The right to inspect and review the student's education records within 45 days after the day the [Name of school ("School")] receives a request for access.

   Parents or eligible students should submit to the school principal [or appropriate school official] a written request that identifies the records they wish to inspect. The school official will make arrangements for access and notify the parent or eligible student of the time and place where the records may be inspected.

2. The right to request the amendment of the student's education records that the parent or eligible student believes are inaccurate, misleading, or otherwise in violation of the student's privacy rights under FERPA.

   Parents or eligible students who wish to ask the [School] to amend a record should write the school principal [or appropriate school official], clearly identify the part of the record they want changed, and specify why it should be changed. If the school decides not to amend the record as requested by the parent or eligible student, the school will notify the parent or eligible student of the decision and of their right to a hearing regarding the request for amendment. Additional information regarding the hearing procedures will be provided to the parent or eligible student when notified of the right to a hearing.

3. The right to provide written consent before the school discloses personally identifiable information (PII) from the student's education records, except to the extent that FERPA authorizes disclosure without consent.

   One exception, which permits disclosure without consent, is disclosure to school officials with legitimate educational interests. A school official is a person employed by the school as an administrator, supervisor, instructor, or support staff member (including health or medical staff and law enforcement unit personnel) or a person serving on the school board. A school official also may include a volunteer or contractor outside of the school who performs an institutional service of function for which the school would otherwise use its own employees and who is under the direct control of the school with respect to the use and maintenance of PII from education records, such as an attorney, auditor, medical consultant, or therapist; a parent or student volunteering to serve on an official committee, such as a disciplinary or grievance committee; or a parent, student, or other volunteer assisting another school official in performing his or her tasks. A school official has a legitimate educational interest if the official needs to review an education record in order to fulfill his or her professional responsibility.

   [Optional] Upon request, the school discloses education records without consent to officials of another school district in which a student seeks or intends to enroll, or is already enrolled if the disclosure is for purposes of the student's enrollment or transfer. [NOTE: FERPA requires a school district to make a reasonable attempt to notify the parent or student of the records request unless it states in its annual notification that it intends to forward records on request.]

4. The right to file a complaint with the U.S. Department of Education concerning alleged failures by the [School] to comply with the requirements of FERPA. The name and address of the Office that administers FERPA are:

    Family Policy Compliance Office
    U.S. Department of Education
    400 Maryland Avenue, SW
    Washington, DC 20202

[NOTE: In addition, a school may want to include its directory information public notice, as required by §99.37 of the regulations, with its annual notification of rights under FERPA.]

[Optional] See the list below of the disclosures that elementary and secondary schools may make without consent.

FERPA permits the disclosure of PII from students' education records, without consent of the parent or eligible student, if the disclosure meets certain conditions found in §99.31 of the FERPA regulations. Except for disclosures to school officials, disclosures related to some judicial orders or lawfully issued subpoenas, disclosures of directory information, and disclosures to the parent or eligible student, §99.32 of the FERPA regulations requires the school to record the disclosure. Parents and eligible students have a right to inspect and review the record of disclosures. A school may disclose PII from the education records of a student without obtaining prior written consent of the parents or the eligible student –

- To other school officials, including teachers, within the educational agency or institution whom the school has determined to have legitimate educational interests. This includes contractors, consultants, volunteers, or other parties to whom the school has outsourced institutional services or functions, provided that the conditions listed in §99.31(a)(1)(i)(B)(*1*) - (a)(1)(i)(B)(*2*) are met. (§99.31(a)(1))

- To officials of another school, school system, or institution of postsecondary education where the student seeks or intends to enroll, or where the student is already enrolled if the disclosure is for purposes related to the student's enrollment or transfer, subject to the requirements of §99.34. (§99.31(a)(2))

- To authorized representatives of the U. S. Comptroller General, the U. S. Attorney General, the U.S. Secretary of Education, or State and local educational authorities, such as the State educational agency in the parent or eligible student's State (SEA). Disclosures under this provision may be made, subject to the requirements of §99.35, in connection with an audit or evaluation of Federal- or State-supported education programs, or for the enforcement of or compliance with Federal legal requirements that relate to those programs. These entities may make further disclosures of PII to outside entities that are designated by them as their authorized representatives to conduct any audit, evaluation, or enforcement or compliance activity on their behalf. (§§99.31(a)(3) and 99.35)

- In connection with financial aid for which the student has applied or which the student has received, if the information is necessary to determine eligibility for the aid, determine the amount of the aid, determine the conditions of the aid, or enforce the terms and conditions of the aid. (§99.31(a)(4))

- To State and local officials or authorities to whom information is specifically allowed to be reported or disclosed by a State statute that concerns the juvenile justice system and the system's ability to

effectively serve, prior to adjudication, the student whose records were released, subject to §99.38. (§99.31(a)(5))

- To organizations conducting studies for, or on behalf of, the school, in order to: (a) develop, validate, or administer predictive tests; (b) administer student aid programs; or (c) improve instruction. (§99.31(a)(6))

- To accrediting organizations to carry out their accrediting functions. (§99.31(a)(7))

- To parents of an eligible student if the student is a dependent for IRS tax purposes. (§99.31(a)(8))

- To comply with a judicial order or lawfully issued subpoena. (§99.31(a)(9))

- To appropriate officials in connection with a health or safety emergency, subject to §99.36. (§99.31(a)(10)

- Information the school has designated as "directory information" under §99.37. (§99.31(a)(11))

ATTACHMENT S-1
Attachment to Parents' Bill Of Rights
For Contracts Involving Disclosure of Certain Personally Identifiable Information

Education Law §2-d, added by Ch. 56 of the Laws of 2014, requires that a Parents' Bill of Rights be attached to every contract with a third-party contractor (as defined in the law) which involves the disclosure of personally identifiable information (PII) derived from student education records ("Student Data"), or certain teacher/principal information regarding annual professional performance evaluations that is confidential pursuant to Education Law §30212-c ("APPR Data"). Each such Contract must include this completed Attachment to provide specific information about the use of such data by the Contractor.

1. Specify whether this Contract involves disclosure to the Contractor of Student Data, APPR Data, or both.

   ☒ Disclosure of Student Data

   ☐ Disclosure of APPR Data

2. Describe the exclusive purposes for which the Student Data or APPR Data will be used in the performance of this contract.

Vendors will identify 250 students (ages 14-21) per year and collect demographic data such as the start date of service, social security number, date of birth, race, ethnicity, student status, the specific pre-employment transition services (Pre-ETS services) received, and any other elements deemed necessary to report expenditures for the funded activities with students. Pre-ETS services are as follows: Job Exploration Counseling, Work Based Learning, Counseling on opportunities for enrollment in comprehensive transition or post-secondary educational programs, Workplace Readiness Training, and Instruction in Self-Advocacy.

3. Identify any subcontractors or other persons/entities with whom the Contractor will share the Student Data or APPR in the performance of this Contract, and describe how the Contractor will ensure that such persons/entities will abide by the data protection and security requirements of the Contract.

   Subcontractors or other entities with whom the Contractor will share data:

Bidder should specifically list in this section any/all subcontractors that will/may receive data.

- NYSARC, Inc. Erie County Chapter
- Aspire of WNY
- Baker Victory Services
- Deaf Access Services
- Intandem
- Jewish Family Service
- Parent Network
- Resource Center

******Continued on next page

Question 3 continued *- How will the Contractor ensure that such persons/entities will abide by the data protection and security requirements of the Contract.*

People Inc. takes the security of personal data seriously. Our agency has taken the following steps to ensure its partners (subcontractors) are able to meet the standards set forth by ACCES-VR.

1) Each of the partners was chosen, in part, because they are currently approved providers of ACCES-VR-services. They each submitted an Appendix S-1 with their contracts, which was approved by ACCES-VR and is on file.

2) People Inc. asked each of the partners to agree to meet and abide by the standards set forth in Appendix S-1. These agreements were included in the original proposal. Excerpts from these letters are provided below –

The ARC Erie County NY:

The Arc Erie County New York's security measures include:

a. Access to the Data is restricted solely to staff who need such access to carry out the responsibilities of the Contractor under this agreement. Staff are not permitted to share Data with any unauthorized party, subject to immediate dismissal;
b. All confidential Data is stored on computer servers maintained within NYSARC, Inc. Erie County Chapter's computer networks, behind appropriate firewalls;
c. Access to computer applications and Data are managed through user ID/password procedures;
d. Contractor's computer network storing the Data is scanned for inappropriate access through an intrusion detection system. NYSED has the right to perform a site visit to review the vendor's security practices if NYSED feels it is necessary;
e. NYSARC, Inc. Erie County Chapter has a disaster recovery plan that is acceptable to the State; and,
f. Satisfactory redundant and uninterruptible power and fiber infrastructure provisions.

Aspire of WNY:

Aspire of WNY agrees to the provisions in Appendix S-1 related to protecting Student Data or APPR in the performance of this Pre-EMTS project. Aspire of WNY has provided a copy of our data protection and security policies to demonstrate our ability to comply with the expectations of ACCESS-VR.

1. Aspire's corporate compliance and IT department regularly ensure staff have the knowledge and ability to encrypt emails. Annually, staff receive mandatory training on HIPAA and general data protection.
2. Aspire's IT system stores data on virtual servers that are backed up daily. All server and email access are protected by Sophos firewall, updated in late 2018.

******Continued on next page**

Question 3 continued *- How will the Contractor ensure that such persons/entities will abide by the data protection and security requirements of the Contract.*

Baker Victory Services:

Baker Victory Services agrees to the provisions in Appendix S-1 related to protecting Student Data or APPR in the performance of this Pre-ETS project. Baker Victory Services has provided a copy of our data protection and security policies to demonstrate our ability to comply with the expectations of ACCESS-VR.

1. All internal case notes are documented in Therap
2. ACCES-VR required reporting forms are kept on a secured network
3. Outgoing emails are encrypted
4. BVS regularly updates security features of the network

Deaf Access Services:

DAS agrees to the provisions in Appendix S-1 related to protecting Student Data or APPR in the performance of this Pre-EMTS project. We utilize the same protocols and systems as People Inc to ensure data protection and security.

Intandem

Intandem agrees to the provisions in Appendix S-1 related to protecting Student Data or APPR in the performance of this Pre-EMTS project. Intandem has provided a copy of our data protection and security policies to demonstrate our ability to comply with the expectations of ACCESS-VR.

Intandem's policy is attached on page 68.

Jewish Family Services

Jewish Family Service of Buffalo and Erie County agrees to the provisions in Appendix S-1 related to protecting Student Data or APPR in the performance of this Pre-ETS project. Student data and/or APPR data will be stored in locked offices (and in locked cabinets) and/or on password-protected devices. Electronic data at Jewish Family Service is encrypted both in motion and at rest. Additionally, data security practices are consistent with Appendix R of this RFP.

Parent Network:

The Parent Network agrees to the provisions in Appendix S-1 related to protecting Student Data or APPR in the performance of this Pre-ETS project. Parent Network's electronic data will be stored in the agency's Data Management System – Salesforce, which is a secure cloud based, encrypted data management system. Hard files will be kept in a locked file cabinet utilizing a standard double lock security system.

******Continued on next page

Question 3 continued *- How will the Contractor ensure that such persons/entities will abide by the data protection and security requirements of the Contract.*

Resource Center

The Resource Center agrees to the provisions in Appendix S-1 related to protecting Student Data or APPR in the performance of this Pre-EMTS project. The Resource Center has provided a copy of our data protection and security policies to demonstrate our ability to comply with the expectations of ACCESS-VR.

All data is stored in Therap Services infrastructure. A number of sources are referenced by Therap to develop the security program, most notably HIPAA. Other key sources include various NIST publications (SP 800-53, et al), industry entities such as HITRUST, CHIME, SANS, and RSA. At Therap, emphasis is placed upon the confidentiality, integrity and availability of the services (and associated data) provided to customers. The network and computing infrastructure that has been designed and developed to deliver these services is assessed on an ongoing basis to ensure compliance with the stated goals. This is accomplished by a combination of physical, technical and administrative controls, as well as ongoing research to identify and address updates to recommended best practices. Multiple mechanisms and controls are in place to ensure the safety and availability of the platform. Some controls enable Therap to control access to platform components, monitor both access and attempted access activities, and address issues that could compromise the integrity of the platform. Other controls are implemented with the objective of maximizing platform reliability, by proactively identifying events or trends that could threaten availability or performance requirements.

Examples of Technical Controls include:

- *Routers and Firewalls*
- *Network Segmentation*
- *Anti-Malware*
- *Load Balancers*
- *Hardened Configurations*
- *Centralized Logging and Event Monitoring*
- *Third Party Vulnerability Assessments*
- *Self-Performed Vulnerability Assessments*

In the event the Contractor engages a Subcontractor or otherwise shares Student Data or APPR Data with any other entity, Contractor acknowledges and agrees that before any such data is shared with a Contractor or another entity, such party must agree in writing to be bound by the confidentiality and data protection provisions set forth in this Contract including, but not limited to, the "Data Security and Privacy Plan" set forth in Appendix R. Upon termination of the agreement between the Contractor and a Subcontractor or other entity, Contractor acknowledges and agrees that it is responsible for ensuring that all Student Data or APPR Data shared by the Contractor must be returned to Contractor or otherwise destroyed as provided in Paragraph 4 of the "Data Security and Privacy Plan" set forth in Appendix R.

4. Specify the expiration date of the Contract, and explain what will happen to the Student Data or APPR Data in the Contractor's possession, or the possession of any person/entity described in response to Paragraph 3, upon the expiration or earlier termination of the Contract.

Contract expiration date: **12/31/24**

☐ Contractor agrees to return the Student Data or APPR Data to NYSED consistent with the protocols set forth in Paragraph 4 of the "Data Security and Privacy Plan" set forth in Appendix R.

☒ Contractor agree to securely destroy the Student Data or APPR Data consistent with the protocols set forth in Paragraph 4 of the "Data Security and Privacy Plan" set forth in Appendix R.

5. State whether the Contractor will be collecting any data from or pertaining to students derived from the student's education record, or pertaining to teachers or principals' annual professional performance evaluation pursuant to the Contract, and explain if and how a parent, student, eligible student (a student eighteen years or older), teacher or principal may challenge the accuracy of the Student Data or APPR data that is collected. ***NYSED program office checks applicable box(es).***

☒ Student Data

☐ APPR Data

Any challenges to the accuracy of any of the Student Data or APPR Data shared pursuant to this Contract should be addressed to the school, educational agency or entity which produced, generated or otherwise created such data.

6. Describe where the Student Data or APPR Data will be stored (in a manner that does not jeopardize data security), and the security protections taken to ensure that the data will be protected, including whether such data will be encrypted.

Bidder should detail in this section where data will be stored, what security measures will be in place, and whether electronic data is encrypted in motion and/or at rest.

People Inc.'s IT and data security policies and procedures are attached on pages 60 - 66

People Inc.'s IT and Data Security Policy and Procedures

Risk Analysis

The agency has numerous departments and systems that contain electronic Private Health Information (ePHI). It has been determined that the responsibility of privacy and security lies within the management of our workforce.

All employees with network access have been instructed to store all data on a network drive, if available. Data should not be stored on a computer's local hard drive (C: D: E:) or on any type of "removable" media. Removable media would be floppy diskette, CDROM, DVD, tape, or flash drives. If you must store data on:

- a local hard drive, it is recommended that the data be encrypted.
- removable media, it is recommended that the data be encrypted and the media must be kept in a locked container or cabinet.

Risk Management

The agency network is connected to the Internet. To help maintain a secure network, and minimize exposure to risks from outside the agency, we have employed the following security measures.

a **Firewall** is in place between the internal network and the Internet. The firewall has been configured with a demilitarized zone (DMZ). This DMZ is a small subnetwork that sits between a trusted internal network (our corporate network) and an untrusted external network (the Internet).

The only servers residing in the DMZ are "front end" servers. Front end servers contain no ePHI data and only act as a gateway device for requesting information from servers containing data on the internal network.

A signature based **Intrusion Detection System** (IDS) has been installed and monitors our Internet connection and the DMZ for suspicious activity. This system will monitor network traffic, looking for known signatures of malicious software or hacking procedures. The system will automatically respond to anomalous or malicious traffic by taking action to block the user or source IP from accessing the network.

All servers residing in the DMZ also run **Secure Agent Software** (SAS). Secure agent software prevents malicious behavior before it can occur by removing potential and unknown security risks based upon behavioral analysis.

The agency also employs a **VPN\Security Management Solution** (VMS). The VMS provides a comprehensive solution that ties separate security and VPN technologies into a single secure network, including Virtual Private Network concentrator, firewall, IDS, and SAS systems.

Sanction Policy

It is the policy of the agency that employees who fail to comply with the security policies and procedures may face disciplinary action up to, and including termination of employment.

Information System Activity Review

The Information Technology department will perform periodic reviews and test security functions based upon internal logging capabilities within the network operating system and the VMS system.

Assigned Security Responsibility

The agency has both a HIPAA Privacy Officer and a HIPAA Security Officer

Authorization and/or Supervision

It is the agency policy that an authorized, knowledgeable person must support vendors whenever work is being done on a system that contains or processes electronic PHI.

Personnel Clearance

It is the policy of People Inc. that supervisors must approve employee access to electronic PHI.
To obtain a network user ID, an employee's supervisor must submit a completed network account form to the I.T. department.

Termination Procedures

It is the policy of People Inc. that when an individual's employment has been terminated, the supervisor will submit a network account form to the Information Technology department revoking access to the network. The supervisor is also required to inform the Facility Management department so that building access will be revoked by disabling the individual's key card. (if applicable)

Access Authorization

It is the policy of People Inc. that an employee's supervisor must approve employee access to electronic PHI. The supervisor will then submit a written or electronic request to the Information Technology department. The Information Technology department will add or remove access as requested.

Access Establishment and Modification

It is the policy of People Inc. that an employee's supervisor must periodically review an employee's access to electronic PHI and submit a written or electronic request to the Information Technology department to change an employee's access.

Security Reminders

The agency is in the process of creating an online training program to education employees on computers and security. The Information Technology department will continue to provide security reminders to staff using various methods, such as email, the Champion program, newsletters, and Intranet.

Protection from Malicious Software

All People Inc. computers that have access to electronic Private Health Information (PHI) are equipped with antivirus software. The software is setup to automatically apply updates on a daily basis with no user intervention and is also setup to scan ALL incoming and outgoing files. It is forbidden for employees to turn off, uninstall, or disable the anti-virus protection in anyway.

The agency has contracted with a vendor to tighten restrictions on the firewall. In the event a workstation is infected by malware, the malware will have limited ability to make contact outside the agency before its presence has been detected.

Log-in Monitoring

The agency will enable auditing features on the Windows-based servers that will track user logins, user attempted logins, and file access. After 3 unsuccessful attempts within a short period of time, the network will automatically disable the user ID for 30 minutes. This is a security measure automatically performed by the network to thwart any unauthorized access to the network.

Password Management

Every user will require a unique user ID and password. IDs and the corresponding passwords **cannot** be shared between 2 or more people, this includes supervisor & subordinate. IDs and passwords should not be written down or posted where anyone else has access to them. The only time you should ever disclose your password, is if it is requested by a member of the I.T. staff to login\test\troubleshoot\repair your computer. If you are required to provide your password to a member of the I.T. staff, you are required:

1.) to be with the person while work is being performed on your computer
2.) to immediately change your password once the I.T. staff is finished working on your computer.

User IDs must be disabled if:

1.) they are currently not in use
2.) an employee has left the agency
3.) an employee is on an extended leave.

Response and Reporting

The Information Technology department will check audit logs from the network operating system and the VMS system. The I.T. department personnel will respond to security incidents, document any incidents and the outcome.

Data Backup Plan

Every network containing ePHI is backed up to magnetic tape 5 days a week. (Monday through Friday). The backup software will email a report of the backup activity, successful or unsuccessful, to an I.T. staff member. The daily tapes, Monday through Thursday, are rotated weekly. There are 5 Friday tapes, rotated monthly, and the Friday tape is sent for offsite storage the following Monday.

The tapes are stored in a media safe in a computer room that is kept secure. To minimize the loss of data due to a disaster, each site sends one tape per week to another site for offsite storage. The data on the tape will be kept secure by password. The data will not be able to be restored without knowing the password, having the appropriate tape unit, and the necessary software.

Disaster Recovery Plan

The agency is in the process of creating a new disaster recovery plan, which will be completed by December 31, 2005. Currently, the agency backs up all software on our network to tape, stores the tapes in a media safe, and 1 tape from each site is stored at another site.

Emergency Mode Operation Plan

In the event of a disaster, the agency will move critical operations to another location. Since data tapes are stored offsite, agency personnel will work with a vendor to acquire the necessary hardware and begin the process to restore operations at a new location.

The agency does not have a formal disaster plan, but one will have a completed plan by December 31, 2005.

Testing and Revision Procedures

The agency will periodically test and verify its contingency plans and revise it as necessary.

Applications and Data Criticality Analysis

It is the policy of the agency that all agency software on a network is backed up to tape. In the event of a disaster, the agency will restore the data to servers that are currently kept as available spares. If enough servers are not available, the agency will acquire servers from our vendors.

Periodic Technical & Non Technical Evaluation

It is the policy of the agency that a periodic technical and non-technical evaluation will be conducted to audit the effectiveness of the security controls and measures in place in consideration of environmental or operational changes.

Business Associates & Other Arrangements

It is the policy of the agency that business associates must be contractually bound to protect electronic PHI as required in applicable federal regulations. It is also the policy of this organization that business associates who violate their agreement will be dealt with first by an attempt to correct the problem, and if that fails by termination of the agreement and discontinuation of services by the business associate. It is the policy of this agency that any business associate agreement that cannot be terminated, and has not corrected the violation will be reported to the Secretary of the Department of Health and Human Services.

Unique User Identification

Every user will require a unique user ID and password. IDs and the corresponding passwords **cannot** be shared between 2 or more people, this includes supervisor & subordinate. IDs and passwords should not be written down or posted where anyone else has access to them.

Certain software within the agency may not provide the ability to assign a unique user ID or have an auditing feature. The agency will evaluate the software and determine a suitable replacement that fulfills our requirements.

Emergency Access Procedure

In the event of an emergency, some records may be available in a non-electronic format, such as our article 28 clinic. Information that is stored only in electronic format, will be restored from tape. Tapes are kept in a media safe, with 1 tape \ week stored offsite.

Automatic Logoff

The agency has determined that the automatic logoff feature is not currently necessary. The agency currently has software applications that do not function well when Windows automatically end sessions.

It has been determined that we can successfully secure the computers by instructing users to “Lock” their Windows workstations whenever they leave the computer.

Encryption and Decryption

The agency has determined that all ePHI is to be stored on Windows 2003 servers running the NT File System. It has been decided that any further encryption would be unnecessary in our situation. All workstations that have access to ePHI are running a secure Operating System, such as Windows XP. Employees have been directed to “Lock” there OS whenever they leave their workstation.

If there is a need to transmit ePHI outside of the agency email system, the email should be encrypted.

The agency does have employees using PDA units that can access the agency email system by a wireless carrier. The PDA unit communications over the wireless carrier, so the data is encrypted using GoodLink Encryption software.

Audit Controls

The agency will enable auditing features on the Windows-based servers to track user logins, user attempted logins, and file access. The Information Technology department will perform periodic reviews and test security functions based upon internal logging capabilities within the network operating system and the VMS system.

Integrity

It is the policy of People Inc. that supervisors will determine who should have access to systems containing ePHI. Employees will only be assigned the minimum rights necessary to perform their job function. The department supervisor should institute procedures to verify the data integrity of applications containing ePHI. The Information Technology Department will perform periodic reviews of the audit logs and test security.

Person or Entity Authentication

Person or entity authentication is done by user ID, where applicable. Remote sites access the agency network over a broadband connection using a secure VPN with 3DES encryption (168 bit). Software VPN clients establish a secure connection using both a user name and group name. Once connected to the VPN concentrator, the user is required to authenticate to the Windows server before being granted access to any ePHI.

Integrity Controls

Information transmitted outside the agency network will be transmitted directly by modem or by the Internet. In the event such data is transmitted over the Internet, it will be done using a high-grade encryption using Secure Socket Layer.

Encryption

In the event any data is transmitted outside the agency using the Internet, the agency will employ a high grade encryption using Secure Socket Layer.

Contingency Operations

In the event of a disaster, the agency will move critical operations to another location. Since data tapes are stored offsite, agency personnel will work with a vendor to acquire the necessary hardware and begin the process to restore operations at a new location.

The agency does not have a formal disaster plan, but one will have a completed plan by December 31, 2005.

Facility Security Plans

The agency has a visitor policy in place. All visitors must sign in at the reception desk. Visitors are accompanied by

an employee when moving about the building.

Access Control & Validation Procedures

It is the policy of People Inc. that supervisors determine a subordinates access priveledges at agency facilities. The agency has facilities that are equipped with Card Entry Systems. Employees are only given access to facilities as per their supervisor's authorization.

Maintenance Records

The Facilities Management department documents any repairs and modifications to the physical components of a facility, including those related to security.

Workstation Use

All workstations should be setup so that unauthorized persons cannot easily see the display. If you are unable to setup your workstation so that others cannot easily see the display, it is required that your purchase and install a privacy screen.

Workstation Security

All workstations within the agency that access ePHI are running secure operating systems, such as Microsoft Windows XP. The computers also authenticate to Windows Active Directory.

Workstation is defined as "an electronic computing device, for example, a laptop or desktop computer, or any other device that performs similar functions, and electronic media stored in its immediate environment." Thus PDAs, tablet computers, and other portable/wireless devices are included.

Any devices that have the ability to access or store ePHI must be kept secure. All computers must be logged off when the employee will not be using the workstation for more than 1 hour. If an employee must leave their workstation, the unit should be logged off or "Locked". The easiest way to lock Windows XP is by simply pressing the **Windows logo key** and the letter **L** (for Lock) on a Microsoft Natural Keyboard or any other compatible keyboard that includes the **Window** key.

Laptop units are allowed to be taken offsite, as long as the units are running a secure operating system (Windows XP) and they have encryption software (SafeBoot) installed. All laptops will be using encryption software (SafeBoot) that requires user authentication before allowing anyone to even login to the laptop.

ePHI should not be stored on any personal digital assistant (PDA) device other than an agency issued PDAs with GoodLink software. GoodLink enable PDAs have the ability to receive internal email that may contain ePHI.

If an employee has a Treo650 that is lost or stolen, the employee should report this immediately to the HIPAA security officer. The HIPAA security officer will then initiate a command to erase ALL information on the PDA.

Disposal

If any computers are to be discarded or donated to another agency, the hard drive must either be erased using a "Wipe" program or the hard drive removed and disassembled.

Media Re-use

All removable media must be reformatted before being reused or destroyed before being discarded. If the media is unable to be reformatted i.e.) CDROM, it must be destroyed by a shredder or broken into multiple pieces.

Accountability

All computer equipment is installed or removed by Information Technology personnel. If the Information Technology department disposes of computer equipment, the hard drives are erased by a "wiping" software or the hard drives are disassembled.

The agency keeps track of its computer equipment using an inventory database application. All disposed equipment is recorded in the database.

Data Backup & Storage

The agency has determined it is not necessary to backup workstations before they are moved. Agency workstations primarily contain an operating system and any applications. Data is not to be stored on computer workstations hard drives. If a user decides to store data on a workstation, it is the user's responsibility to make copies of the data on a secure removable media.

INTANDEM
people | purpose | progress

Technology & Communications Resources

Usage Policy

This policy applies to Intandem ("Agency") and Opportunities Unlimited of Niagara Foundation, Inc. ("Foundation").

The policy applies to all ("Individuals") Agency employees, consultants and individuals who have been authorized by the Director of Technology and Communications, to access Agency Technology and Communications Systems.

Technology and Communications Systems ("Information Systems") include but are not limited to computer hardware and software, computer peripherals, telephone systems, projections systems, network hardware and cabling.

AGENCY STANDARDS

The CIO, in partnership with the Department of Technology and Communications, and the Department of Informatics, is responsible for defining the standards applicable to Agency wide computer information systems. These standards are required to insure a consistent technology base that remains compatible with the Agency's overall technology and communications architecture, and to insure that provided technological resources are used in an appropriate manner.

Use of personally owned computer hardware, computer software, peripherals, cell phone cameras, cameras, video and audio recorders, without authorization within any Agency premises is prohibited. This includes the installation and use of any personally acquired or developed computer software on Agency computer equipment. Periodically, the Technology and Communications department will conduct a site audit to monitor computer usage and performance, general system status and condition, and installed applications and operating systems. Vendor software contracts and licenses are very explicit and violations expose the Agency to severe fines and penalties. The installation of personally owned software may also expose the computer, or network to the introduction of a virus. Any employee violations to this policy will be confidentially reported to the employee's supervisor for appropriate disciplinary action.

Physical movement of computing equipment must be coordinated by the Technology and Communications Department.

Confidentiality

During the course of their employment/work activity, individuals may encounter confidential information, particularly through the use of Agency information systems. Such confidential information may include, for example, consumer data records, employee compensation and other financial information. Individuals shall not access, acquire, use, copy, or transfer confidential information except to the extent necessary to fulfill their employment duties/work activities. Persons who exceed their authority in using confidential information or who gain access to such information through unauthorized means, including the use of Agency information systems, should realize that their conduct is in violation of the Agency's confidentiality policy, as well as this policy statement and will be dealt with accordingly. Such conduct may also be in violation of state and federal law and may subject such persons to the appropriate penalties.

Individuals shall take all appropriate action, whether by instruction, agreement, or otherwise, to insure the protection, confidentiality and security of confidential information. The obligations of an individual to maintain the confidentiality and security of confidential information survives the termination of the individual's working relationship with the Agency.

Acquisitions

All acquisitions of technology and communications products, including software, hardware, and supplies must be ordered through the Purchasing Department and approved by the CIO in partnership with Department of Informatics and/or Technology and Communications, accompanied by proper manager approval. In the case of large, applicable expenditures, the Agency's Capital Request process must be followed.

Software

The combination of software products and internally written program instructions constitute a 'system'. An example of a system is a database developed in Microsoft Access. System requirements and potential benefits must be reviewed by the Informatics department to insure the integrity of the Agency's overall computing architecture. Systems will be developed by assigned information systems personnel. Information, data, and programs generated by, or stored in, computing devices are Agency assets and the property of Intandem. As such, it is prohibited to offer for sale, or to provide any Agency program/software application, whether purchased from a third party vendor or developed internally by the Informatics department, to any outside individual, business entity, or organization.

Programs and software applications developed internally by information systems department staff require a significant amount of labor during the analysis, design, installation, implementation and training phases of development. In most cases, this expense is much greater than the cost of purchasing an application from a third party provider. These Agency assets are only available for sale, or provided for use by any outside party(s) at the sole discretion of Agency management and are not to be shared, or given to others, casually.

User Account Passwords

User accounts, along with their associated passwords, are the means by which information is protected from unauthorized access. As a result, the proper selection and protection of a password are very important. The individual to whom a user account is issued is responsible for all activity on that account. Proper password security helps insure that others do not misuse an account for which you are responsible. Passwords on user accounts must not be shared, unless authority and approval to do so is given according to the process outlined the Agency HIPAA Security Guide § 3.2, 3.3, 4.1 and 4.2. If at any time you feel that your password and account has been compromised, contact the Software Systems Manager or Director of Technology and Communications immediately, to have it changed.

Virus Protection

Computer viruses are destructive programs, or computer instruction sets, that can, in some cases, render a PC or entire network unusable through the corruption of data files or the operating system, itself. Many of these viruses are almost undetectable at their introduction to the computer. They may remain 'dormant' for a period of days, weeks or even months before they manifest themselves, at which time it may already be too late to save a significant amount of data and probably will have been spread to other user PC's and network equipment.

It is each individual's responsibility to guard against the introduction of a computer virus. This will be accomplished by utilizing the virus protection software installed on each computer. As new viruses are developed and deployed on a routine basis, the virus protection software may become outdated, however it may still be able to recognize the existence of a virus and alert the user to this fact. The Technology and Communications department will take all cost effective measures to maintain the virus protection software at the most current level of virus recognition, on a routine basis.

There are many ways that computer viruses can be introduced and spread across many PC's. The most common method of introduction and spread of these viruses are the sharing of data files on removable devices (diskette, CD's, thumb drives, etc) or shared network directories, between users, and internet email attachments. It is required that each user ensures that automatic virus protection remains turned on at all times so all discs, files and emails with attachments are scanned on a real-time basis. If a virus is detected, the virus protection software should be utilized to destroy it. If the software cannot destroy the virus, it will most likely report the existence of it. In any case, the user should make note of the reported virus, where the file(s) containing the virus came from, and contact the Director of Technology and Communications, immediately. We can then track the virus down and hopefully eliminate it very quickly, before any severe damage takes place.

Any individual(s) willfully and knowingly designing, writing, copying a computer virus, or other program, or code, of a destructive nature, to introduce, or spread to any Agency computer or computer system is in violation of this policy and will be subject to Agency disciplinary action. Such conduct may also be in violation of State and/or Federal law and may subject such persons to the appropriate penalties.

TECHNOLOGY AND COMMUNICATIONS SYSTEMS USAGE POLICY

The Agency's information systems are provided for the use of Agency management, staff and approved individuals, in support of the programs of the Agency. All individuals are responsible for seeing that these information systems are used in an effective, efficient, ethical, lawful manner. The use of information systems is a privilege, not a right, which may be revoked at any time for misuse. The following policies relate to their use.

The information systems are owned by the Agency and are to be used for Agency related activities only. All access to shared, networked information systems, including the issuance of accounts, must be approved and established through the Technology and Communications department.

Information systems are to be used only for the purpose for which they are assigned and are not to be used for commercial purposes or non Agency related activities.

Electronic files (including electronic mail, computer files and voice mail) are presumed to be private and confidential Agency property. Their contents may be accessed only by authorized personnel for compelling business or security reasons.

Fraudulent, harassing, slanderous, offensive or obscene messages or materials are not to be sent, printed,

requested, displayed or stored on Agency owned or operated information systems. Agency information systems resources should not be used in a manner that would embarrass or bring discredit to the Agency in the view of their constituencies. Chain letters and other unauthorized forms of mass mailings are not allowed. Derogatory or inflammatory information such as a picture or information about a person or business entity is not to be made publicly available, such as on web pages or screen savers, etc.

An individual to whom the Agency has provided access to one or more of its information systems may not permit another person to use the system(s) except as outlined in Agency HIPAA Security Guide § 3.2, 3.3, 4.1 and 4.2. An individual to whom the Agency has provided access to one or more of its information systems is responsible for the proper use of the resource, including proper password protection.

Special software may be installed on Agency information systems in order to support resource usage accounting, security, network management, back up systems and software updating functions, and to provide better support to personnel. Authorized information systems personnel may access others files when necessary for the maintenance and security of information systems. When performing maintenance, every effort will be made to insure the privacy of a user's files. However, if violations of policies are discovered, they will be confidentially reported to the employee's supervisor for appropriate action.

No unauthorized person may alter an Agency information system. The use of loop holes or specific tools to circumvent information systems or network security, the knowledge of special passwords, or the covert acquisition of passwords to damage information systems, obtain extra resources, take resources from another user, or gain access or control of any system for which proper authorization has not been granted is expressly prohibited.

Software and other materials licensed to the Agency, other business entities, or persons may be protected by copyright, patent, trade secret, or another form of legal protection ("protected materials"). Protected materials may not be copied, altered, transmitted, or stored using Agency owned or operated information systems, except as permitted by law or by the contract, license agreement, or express written consent of the owner of the protected materials. The use of software on a local area network or on multiple computers must be in accordance with the license agreement. Software use can only be authorized by the CIO in partnership with the Technology & Communications department or Department of Informatics and the use of unauthorized software on any Agency information system is prohibited.

An individual's information systems usage privileges may be suspended immediately by the Director of Technology and Communications or Software Systems Manager upon the discovery of a possible violation of this policy. Such suspected violations will be confidentially reported to the appropriate supervisor.

A violation of this policy will be dealt with in the same manner as a violation of other Agency policies and may result in a disciplinary review. In such a review, the full range of disciplinary sanctions is available, including the loss of information systems usage privileges, dismissal from the Agency and possibly, legal action.

Internet Usage Policy

Overview

Access to the Internet is provided as a tool to help you do your job. We are pleased to be able to offer Internet access to selected staff. While access to the Internet provides many benefits it also has the potential to create significant risks to the Agency. Inappropriate Internet usage may result in lost employee productivity, loss of confidential data, legal liability, negative publicity, and exposure to virus attacks and/or excessive cost to Intandem. This policy states Intandem's expectations regarding Internet use. It is being provided to help you understand the difference between acceptable and unacceptable Internet activity. All Agency Internet users should review this policy carefully and comply with it at all times. The term "users," as used in this policy, refers to all employees, volunteers, independent contractors and other persons accessing or using Intandem's computer systems. This policy applies to all users when they are using computers or Internet connections supplied by Intandem, whether or not during work hours, and whether or not from the Agency's premises.

Key Points

1. Access to the Internet is provided in order to help you perform your job. We expect you to use the Internet for work related purposes only.
2. Anything you do while using the Internet will be monitored by Intandem. Sites visited by each employee are continually and automatically logged and the log is maintained and periodically audited. We reserve the right to inspect and monitor Internet use and all files stored on any Agency system. We reserve the right to limit or block sites that may be accessed on the Internet. Excessive Internet traffic will adversely affect all computer systems, e-mail systems and telephone systems throughout the Agency.
3. We require that you conduct yourself honestly, legally and appropriately on the Internet. All existing Agency policies apply to your conduct on the Internet, especially (but not exclusively) those that deal with safeguarding resources, confidentiality, plagiarism, corporate compliance, sexual harassment and community relations.
4. Use of the Internet for illegal activity is grounds for immediate termination for employees and we will cooperate with any legitimate law enforcement activity.
5. Individuals will be held accountable for any breaches of security or confidentiality while using the internet.

Examples of proper Internet use include but are not limited to:

1. Communicate and exchange information directly related to the mission and work tasks of Intandem.
2. Research relevant topics related to the Agency mission.
3. Obtain information for grants, fundraising and to promote Agency events.
4. Access state contract information and communicate with vendors and suppliers.
5. Research new product lines and find new subcontract customers for Workshop functions.

6. Access Medicare, Medicaid, and other government and regulatory agencies that we conduct business with.
7. Access financial institutions such as Key Bank that we conduct business with to obtain and transmit necessary financial information.
8. Communicate with Agency insurance carriers.
9. Communicate with professionals in related fields. NO INSTANT MESSAGING of any kind is allowed!
10. Recruit qualified applicants and post open positions.

Unacceptable uses of the Internet include but are not limited to:

1. Store, view, print or redistribute any document or graphic file that is not directly related to the user's job or the Agency's business activities.
2. Display, transmit or record any information, which is defamatory, false, inaccurate, abusive, threatening, obscene, racially offensive, or discriminatory.
3. Violate agency policy prohibiting sexual harassment.
4. Conduct or promote any illegal activity or misuse any Agency assets or resources.
5. Access, upload, display, transmit or distribute sexually explicit or obscene material.
6. Download or distribute pirated software or data.
7. Download or duplicate copyrighted material without permission.
8. Download entertainment software, iTunes, music or games, or play online radio stations, music or games over the Internet.
9. Download images or videos unless there is a specific business-related use for the material.
10. Upload any software licensed to the Agency or data owned or licensed by the Agency without specific authorization from the manager responsible for the software or data.
11. Speak/write in the name of the Agency in any electronic communications, unless you are authorized to speak at public gatherings on behalf of the Agency.
12. Engage in any activity for personal gain or conduct personal business transactions.
13. Make any unauthorized purchases.
14. Deliberately distribute any virus, worm, Trojan horse or trap-door program code.
15. Reveal confidential Agency information, customer data or any other material covered by existing Agency Confidentiality policy.

Procedure for Obtaining Internet Access

1. A supervisor may request the Director of Technology and Communications for internet access for an employee for legitimate and necessary Agency activity.
2. Upon access to the Internet, the supervisor will orient the employee on the Internet Usage Policy which will be stored in the Agency's Electronic Library.

Privacy

You have no privacy while using the Internet. Intandem will monitor Internet use. All Internet messages and other communication composed, sent or received is the property of Intandem. We have systems in place that are capable of tracking and monitoring every Internet site that you visit. Internet usage reports will be reviewed and may be publicized in order to ensure compliance with Agency policy.

The Agency uses software that identifies inappropriate or sexually explicit web sites. We will block access from within our network to inappropriate sites that we are aware of. If you accidentally connect to a site that contains sexually explicit or offensive material disconnect from it immediately.

Inappropriate Communications and Confidentiality

The use of any instant email services or instant-messaging services is strictly prohibited due to inherent vulnerability and security risks.

One of the most valuable uses of the Internet is to obtain and share information with individuals in our line of work. News groups, forums, bulletin boards, chat rooms and user groups related to developmental disabilities allow for interactive two way communication with others in our field. These types of interactive sites may be valuable sources of information. However, these sites can also create opportunities for users to divulge confidential information and make inaccurate or potentially damaging statements about our Agency. If you use an on-line forum you may be perceived as representing the Agency and therefore, we remind users that your correspondence on the Internet should always be accurate, appropriate and related to work. You are not permitted to speak on behalf of the Agency, unless so authorized, and if you express any opinions you must make it clear that they are your own and do not represent the Agency. It is inappropriate to disclose confidential Agency information or any other material covered by existing agency confidentiality policies. Individuals releasing confidential information, whether intentional or not, will be held responsible and subject to any penalties that may result.

Since a wide variety of material may be considered offensive by others it is a violation of Agency policy to store, view, print or distribute any information, document or graphic file that is not directly related to the user's job or the Agency's business activities.

Downloading/Uploading Files

No individual may use agency systems to download pirated software or data, entertainment software or games. Downloading or duplicating copyrighted material is also prohibited. You may only download images, data or files that are directly work related. Everything that you download becomes the property of the Agency.

Software, including shareware and freeware, cannot be installed. Software that is authorized for download must be properly licensed and registered and used only under the terms of its license.

Each file that is downloaded must be scanned for viruses before it is run or accessed.
If you have a work related need to upload (transmit from your computer to a web-site) data or files you must first obtain authorization from both your Program Director and the HIPAA Security Officer.

Security

Intandem has installed Internet firewall and filtering devices. These devices prevent unauthorized access to our computer systems and to web sites deemed unacceptable by the Agency. Any employee who

attempts to disable or circumvent these devices or any other security measures is subject to disciplinary action up to and including termination.

All Agency Internet users must access the Internet through agency-approved gateways.

Questions/Suspected Violations

If you have any questions about this policy or are not sure if something is an appropriate or inappropriate use of the Internet please direct your questions to the Technology and Communications Department. We welcome your questions and want you to ask if you are in doubt rather than proceed and place the Agency at risk.

If you suspect, observe or are aware of any violations of this policy by anyone using our Agency systems report it immediately to your supervisor and the Technology and Communications Department. The misuse of Agency resources or violation of Policies and Procedures could result in the revoking of Internet privileges, disciplinary action and depending on the infraction, could be grounds for immediate dismissal. Violations of State and/or Federal Laws will be reported to proper authorities and the Agency will cooperate in prosecution to the fullest extent of the law.

Email Usage

Rules for Protected Health Information

The transmission of Protected Health Information (PHI) via email, using agency email systems, to other users on our internal network (internal email) is permitted, as long as such transmissions are compliant with the HIPAA privacy rules and other rules and regulations of the Agency and rules of governmental agencies that have jurisdiction over our operations. Internal email is defined as email from an Agency authorized user (a user with a user ID assigned by the Department of Technology and Communications) to any other Agency authorized user on our internal network. The email must be sent from a workstation on the Agency network and directed to an Agency assigned User ID on the network using the internal secure exchange server. The ONLY valid email addresses for the Agency's secured email server is username@oppunlimited.org.

All emails that do not fall under the above definition of internal email are considered external emails. If you need to transmit PHI via external email (assuming such is authorized and does not violate any Agency or Regulatory authority policy, or any HIPAA rule), you must at a minimum place you information inside an encrypted* document, password protected (with a 10 character, high complex password), attached to your email. You must send the password protected document in a separate email. The password would then be sent in a separate email to the same recipient so they may open the password locked document.

NOTE: ALL email addresses with username@opportunitiesunlimited.org are outside unsecure email addresses used in the organization.

*HOW TO ENCRYPT SENSITIVE DATA FOR OUTSIDE E-MAIL

This procedure meets HIPAA and HITECH standards for encrypting data.

1. You should never send PHI or other sensitive information in an open or unencrypted e-mail. Do Not forward sensitive information or PHI from your secure internal e-mail to an unsecure external e-mail address. If you do not understand the difference Please ask!
2. Sending an e-mail to an outside entity has the same security as sending a postcard in the mail.
3. If you must send PHI via unsecure external e-mail you must first put that information in a word document and encrypt that document with the following procedure.
    A. Create a word document with the PHI included. This procedure may be used on an existing word document.
    B. Select the tools tab.
    C. Under tools select the Options tab.
    D. Select the Security tab.
    E. In the "Password to open" box add at least a 10 character password using a combination of upper lower case characters along with numbers and special characters such as !@#$&*. As you increase the total character count with number and special character combinations the more secure the document.

F. After you have typed the password select the "Advanced" tab next to the password.
G. Select RC4, Microsoft Enhanced Cryptographic Provider v1.0. Make sure the Choose a key length: is set for 128 and then select the OK tab.
H. Select the OK tab at the bottom of the Options box.
I. A box will pop up to enter the password from step E above.
J. Save and name your document.
K. Test your document security by opening it. You should be prompted for the security password to open the document. Always test your document for security before sending it.
L. You must send the password in a separate email to your receiving party. NEVER combine the password with the secure document in the same e-mail.

Other Rules

1. Use of the Agency's email system should be mainly confined to Agency related business. Occasional email not related to the Agency is acceptable as long as it is occasional. Personal email received by Agency employees that contain attachments should NEVER be forwarded to other Agency employees and these attachments should NEVER be opened.
2. No agency confidential data may be included or attached to external emails (as defined above) without the approval of an Agency Director.
3. Harassment, sexual or otherwise, whether through language, frequency, or size of messages, is prohibited.
4. Employees may not send email to any person who does not wish to receive it. If a recipient outside of our Agency asks to stop receiving email, the employee must not send that person any further email.
5. Employees are explicitly prohibited from sending unsolicited bulk mail messages ("junk mail" or "spam"). This includes, but is not limited to, bulk mailing of commercial advertising, informational announcements, and political messages. Such material may only be sent to those who have explicitly requested it.
6. Malicious email including, but not limited to, "mail bombing" (flooding a user or site with very large or numerous pieces of email), is prohibited.
7. Forging of header information in any manner is not permitted.
8. E-mail chain letters are strictly forbidden.
9. The Agency's email system should never be used for harassment, profanity/pornography, or personal business activities.
10. The Agency's email system should never be used for distribution of copyrighted materials (including software) or any other illegal activity.
11. Any email messages containing attachments, and received from unknown or unsolicited sources should not be opened and should be brought to the attention of the Department of Technology and Communications immediately. Any virus messages should also be brought to the attention of the Department of Technology and Communications immediately.

Note: Email is distributed through the Agency's servers. All emails are stored on the Agency's server and kept there indefinitely – regardless of a user deleting the message. People should exercise discretion

in using email knowing that email can be retrieved for an indefinite period of time. The server's hard disks are backed up to tape/hard drive nightly. Email sent and received through the internet pass through several servers external to the Agency in addition to our own and thus email messages should not be considered private. The Agency reserves the right to limit the amount of storage available for email messages. The Department of Technology and Communications will monitor email usage for inappropriate usage.

Password and User ID's

Digital information is considered an agency asset and must be appropriately protected against all forms of unauthorized access, use, disclosure, modification or destruction. Information security controls must be sufficient to ensure the confidentiality, integrity, availability, accountability, and audit ability of important information.

Information security controls must be applied in a manner consistent with the value of the information and in accordance with agency HIPAA security policy and any other applicable state and federal regulations. More critical or sensitive information and information technology resources will require more stringent controls.

Procedures

1. Information security controls such as Passwords and User ID's are issued, managed and maintained by the Software Systems Manager and Director of Technology and Communications (TAC).
2. Program Director (or designee) or Human Resources is required to notify the Software Systems Manager and Director of Technology and Communication of a prospective new hire or staff position change whose job responsibilities now require use of agency computers. This notification should occur no less than one week prior to hire or job change. Said employee will be required to have the skills necessary to perform their computer related job functions before being considered for employment.
3. Program Director (or designee) or Human Resources is required to immediately notify, via email, the Software Systems Manager and Director of Technology and Communication of a change of position for an employee or termination of an employee where use of Agency automated systems was required. Upon such notification, security measures will be taken to insure that there is no breach of agency related information and the employee's passwords/ user ID's will be removed from any applicable systems.
4. Any employee, prior to assuming a position which requires use of Agency automated information systems, will prove capability to properly use the hardware and specific software application(s) that are required to access to perform their job responsibilities. This may require formal training. The Software Systems Manager will evaluate the employee's skill level and give approval for assignment of a username and password when the employee has successfully demonstrated proper use of the systems. At that time the (prospective) employee will be assigned individual Password(s) and User ID(s) for all applicable, protected automated system(s)
5. A person to whom the Agency has provided access to one or more of its information systems may not permit another person to use the system(s) except as outlined in Agency HIPAA Security Guide § 3.2, 3.3, 4.1 and 4.2. A person who has been provided access to one or more of the Agency's

information systems is responsible for the proper use of the resource including proper password protection.

6. Any sharing of passwords/user ID's is prohibited and password/ user ID privileges will be revoked if such activities are found true.

An individual's information systems usage privileges may be suspended immediately by the Director of Technology and Communications or the Software Systems Manager upon the discovery of a possible violation of this policy. Such suspected violations will be confidentially reported to the appropriate Program Director and Executive Director.

A violation of this or related policies will be dealt with in the same manner as a violation of other Agency policies and may result in a disciplinary review. In such a review, the full range of disciplinary sanctions is available, including the loss of information systems usage privileges, dismissal from the Agency and possibly, legal action.

Computer Skills Evaluation

Any employee, prior to assuming a position which requires use of Agency automated information systems, will prove capability to properly use the hardware and specific software application(s) that are required to access to perform their job responsibilities. This may require formal training for use of the Agency's database systems. The Software Systems Manager will evaluate the employee's skill level and give approval for assignment of a username and password when the employee has successfully demonstrated proper use of the systems. At that time the (prospective) employee will be assigned individual Password(s) and User ID(s) for all applicable, protected automated system(s)