Appendix T - Cloud Security Implementation-v1

Cloud Service Provider (CSP) under consideration must demonstrate the ability to comply with local federal and state laws and regulations, specifically Ed Law 2-d.

The following must be addressed for all CSPs under consideration for cloud services and must demonstrate their compliance with applicable security controls. Adjustments can be made in accordance with the type and scope of the cloud service.

DATA

At a minimum, they should adhere to the following, but not limited to:

1. Backup:
    a. In cases where backup is required, all agreements should establish service level agreements
2. (SLAs) for the restoration process including recovery time objective (RTO) and recovery point objective (RPO), and the CSP must demonstrate its ability to meet that SLA, with penalties established for failure to meet SLA.
    a. Where backup is required, private data and its backups must be encrypted in transit and at rest.
3. Data Retention:
    a. Where legal mandates for data retention apply, all agreements must establish terms for preservation, retention, filtering, and retrieval. The CSP must demonstrate its ability to meet the legally mandated requirements.
    b. Even where legal mandates do not apply, the CSP may not delete or remove NYSED data without express permission of the NYSED to do so.
4. Business Continuity: Where Business Continuity/Disaster Recovery (BC/DR) services are required, all agreements should establish terms for BC/DR, and the CSP must demonstrate its ability to fulfill the terms. CSP must provide when requested policies and procedures that address data availability, disaster recovery, data backup and retention.
5. Data Commingling: Data commingling should be prohibited.

IT SECURITY

Cloud providers should be able to demonstrate compliance with current Ed Law 2-d and NYSED Security Policies. At a minimum, they should adhere to the following:

1. Encryption: The use of proprietary encryption algorithms is not allowed for any purpose, unless reviewed by qualified experts outside of the CSP in question and approved by the NYSED Chief Information Security Officer.
2. Incidents:
    a. The CSP should immediately notify the NYSED of any breach of the security of data following discovery of the breach if data was, or is reasonably believed to have been, acquired or accessed by an unauthorized person. The CSP should also notify NYSED Chief Privacy Officer in accordance to SED Law 2-d.
    b. Upon NYSED request, the CSP must supply all logs (including operating system, DBMS/database, and application logs) for the affected host machine.
    c. The CSP should provide a documented incident response plan.
3. Reporting:
    a. The CSP should provide notification of any breach and/or attempted breach in accordance to Ed Law 2-d.

   b. Any history of security breaches or attempted breaches must be disclosed.
4. Risk Management and Compliance – Audit by a certified impartial third party with a focus on reviewing the effectiveness of the implemented security operation controls, have been developed and maintained.
   a. Demonstration that independent audit assurance and compliance have been performed at least annually.
5. Enhancements/Upgrades: The CSP should notify the customer of any changes to the system, such as changes made as enhancements and upgrades, which can impact the security of the system.

SUPPORT

At a minimum, they should adhere to the following, but not limited to:

1. Identity and Access Management:
   a. Have in place and provide when requested policies and procedures that address data flow, data handling, and disposal at a minimum.
   b. Access Control – Required access management policies, practices, and technologies to ensure proper authentication, authorization, auditable and role-based access,
2. Personnel Security:
   a. Screening practices of personnel
   b. Record and tracking of personnel separating from the organization
   c. Record of annual Privacy and Security Awareness Training
3. Monitoring:
   a. The CSP should provide information about monitoring methodology including tools and procedures.
4. Upgrades:
   a. The CSP should give notification of upgrades.
   b. The CSP should outline how testing of upgrades will be performed.