**Compare and Contrast of Information Security Policies**

**State if New Mexico and State of New York**

**Introduction**

The State of New Mexico information policy provides the security to avoid any crash on confidential information of people of New Mexico. The policy comprises all the requirement that all State Entities (SE) shall meet in order to maintain Data Breach on the Internet. It establishes a secure processing base and a stable processing environment. All State government should have information policy that can provide, data security of its people. The data which have the most importance and vulnerability for the common public.

The purpose of the Information policy of the State of New York, to provide effective management to control the risk of security exposure and compromise. The policy assures a secure and stable information technology environment on all SE. The State policy also monitors the system to detect anomalies that might compromise the system.

**Common Principles and Policy Sections**

* **Chief Information officer**

Both the policy dictates that there should be a Chief Information Officer who also serves as the director of the State Office of Information Technology. The Chief Information Officer (CIO) should have all the authorities to oversee, direct and shape the information policy regulations according to the need of time.

CIO have all the responsibilities to examine all aspects of the SE security program, ensures that all periodic SE security assessment are performed. CIO also ensures that confidentiality, integrity, availability and accountability of all SE information is processed through a secure channel and controls guideline, procedure as well as SE security training program (NYS, 2016).

* **Information classification and Handling**

The Information Policy for both of the States includes Information classification and handling which maintain the data processing and handle information. All information that is created or acquired for the business transaction within SE used only by that particular transaction. The information that is collected should come from an authorized resource.

Each classification comprises a set of range of controls designed to protect the value of information and risk of loss. These set of controls also apply to all the application software used to collect the necessary information. The third party who gathered information from SE will have a written consent of CIO before further sharing of information with the fourth party (Jansen, 2011).

* **IT Asset management**

All IT hardware and software designated to business or individuals must be assigned by State Government so that they can be evaluated if any data breach identified. All SE maintain an inventory of hardware and software including system information such as network address, machine name or software version so they can be processed by technical feasibility.

Assets management includes classification which requires the level of protection. The SE documents all the asset by defining the use, copying, storage and transmission of asset and destruction requirement so assets can be handle categorically (NYS, 2016).

* **Account Management and Access Control**

Both of the policies dictates that all accounts must have an individual employee or there should be groups who will be assigned an account to manage. All accounts should be associated with a user-ID and authentication token such password or biometric which identifies the actual user of the account.

The token should not be stored on paper, hand-held device or in an electronic file unless the method of storage is approved by the ISO designated official. Logon banner must be implemented on all the system to inform all the user about the system activities.

* **System Security**

The services that process or store sensitive or confidential information should go through the security technical security review. System securities ensure the transmission of data through a safe channel and avoid any data breach through data transmission.

Any information or process that supports SE business function should be managed properly for information risk assessments and should consider as the part of life cycle. The data this security management detects should be processed and analyzed by technical experts. Risk assessment provides the decision-making tools to manage the risk (NYS, 2016).

**Unique aspects of The State of New Mexico Information Security Policy**

* **Software Maintenance**

To ensure the software accuracy and integrity, all software maintained at a vendor-supported level unless SE CIO approves otherwise. The State of New Mexico information policy provides all New Mexico SE software management. This management includes the latest version of the software and updated version. All changed must be logged so that it should ensure public about the changes have been authorized, tested and accepted by CIO. Any changes made in the software or the upgrading of a software must be under the supervision of CIO and he should be the one who directed those changes in written form (Jansen, 2011).

* **Control of Internal Processing**

The data stored in hardware can be corrupted as the device has been damaged or another malfunction is experienced through processing error. Therefore there should be a check and balance of data processing method so it can be identified when data corruption occurs. The correction program should be introduced to manage the corrupted data and safe the information for the better use. And make sure that if the malfunction is experienced by the device or the source code of the software.

* **Electronic Signature**

The State of New Mexico provides all of its SE a personal way to use the information transaction facility by using an electronic signature. This Electronic signature introduced by the State government through the New Mexico State`s Uniform Electronic Transaction Act. By using this signature each and every SE must have an individual identification that can be used only to transmit the information through one member to another and each member should have one individual electronic signature.

**Unique aspects of The New York State Information Security Policy**

* **Personal Security**

The New York State government information security policy provides it’s all SE workforce general security awareness. The awareness will enable all the SE workforce to recognize, report and analyze the inside threat within 30 days. Personal security provides the maximum security measurement that an individual can enjoy to transmit, share and store information. All job positions must be evaluated by the SE to determine whether they require access to sensitive or sensitive information technology assets. Upon a change of job duties, a process must be established within the SE to review the suitability determination categorically (NYS, 2016).

* **Operations security**

All the systems and the hardware or facilities in which they are stored must be documented according to the SE requirements. Operating instructions, management processes, and incident management procedures that are related to information security should be managed by SE. Approved configuration standards must be used to system configurations. The systems should be maintained at the vendor-supported level which ensures integrity and accuracy. Operations security manages all the tasks that take part in the data gathering and processing which includes data security, limit storage, and the other facilities. The system configuration must be done under the Chief Information Officer (NYS, 2016).

* **Cyber Incident Management**

The State Entities must have incident reports on the data storage and data transmission. If the data transmission have been under threat or can be under the risk so it should be informed to the authorities and New York Information policy provides that facilitation to all its SE. The SE must have incident response plan which should be consistent with the New York State Standards to effectively respond the incident. All observation or suspected information or weaknesses should be reported to the concerned ISO designated representatives. These representatives will analyze the weakness within the system and bring the solution to the fold (NYS, 2016).

**Recommendations**

Each State Information policy has better points and policy sections which provide necessary infrastructure to all its SE to ensure the security of confidential and sensitive information. One other way that both Agencies can use to secure the data and protect the vital information to be compromised is the use of Cloud technology. This can be used as using Cloud as a local server. Cloud computing provides data security to its maximum extent. Users can approach, manage, share and protect their data with maximum security and they will have the full authority to share the information through a proper secure channel.

**Reference**

Jansen, Wayne (2011). Guidelines on Security and privacy in Public Cloud Computing.[WEB] Retrieved form: <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf>

NYS. ITS (2016). New York State Information Technology Policy. [WEB] Retrieved from: <https://its.ny.gov/sites/default/files/documents/enterprise_information_security_policy_v5.1_0.pdf>

Department of information technology (2010). State of New Mexico: Information Security Policy. [WEB] Retrieved from: <http://www.doit.state.nm.us/docs/securityoffice/state_security_policy.pdf>