Security Policy

Matthew Austin

Fontbonne University

Quagliata

23 August 2016

**Data Security Policy: Data at Rest & Data in Motion**

*Using this policy*

This policy defines the security policy for data in motion within Global Telecommunications Company to ensure protection of such data.

*Scope*

This policy applies to all equipment and data owned and operated by Global Telecommunications Company regardless of the environment where the data reside (including cloud systems, servers, personal computers, mobile devices, etc.). The policy applies regardless of the media on which data reside (including electronic, microfiche, printouts, CD, etc.) or the form they may take (text, graphics, video, voice, etc.).

*Definitions*

**Data at Rest**: is the term used for data in computer storage. Data that falls under this category could include files stored on a company's local hard drive, copies of the file stored on onsite and offsite backup tapes and files on the servers of the storage area network.

**Data in Motion:**  is the term used for data as it is in transit. It is the process of the transfer of the data between all of the versions of the original file, especially when data may be in transit on the Internet.

**Encryption:** is the conversion of electronic data into another form, called ciphertext, which cannot be easily understood by anyone except authorized parties. (Secure The Breach)

**Data Monitoring:** is adata monitoring committee (DMC) – sometimes called a data and safety monitoring board (DSMB) – is an independent group of experts who monitor patient safety and treatment efficacy data while a clinical trial is ongoing. (Secure The Breach)

**Data Classification:** Data classification is the process of organizing data into categories for its most effective and efficient use. A well-planned data classification system makes essential data easy to find and retrieve. This can be of particular importance for risk management, legal discovery, and compliance. (Secure The Breach)

***Roles & Definitions (Education of Global Telecommunication)***

Global Telecommunications Company responsibilities of data in rest and motion range in scope from security controls administration for a large system to the protection of one's own access password. Each step is to ensure the protection of all data that is both in rest and in motion owned or associated with Global Telecommunications.

**IT/Administrative Officials must:**

-Identify the electronic information resources within areas under their control.

-Define the purpose and function of the resources and ensure that requisite security education and documentation are provided to the campus as needed which should include password security (for regular users ie. students, teaching staff, etc) and proper key and/or password sharing/security for other IT/Administrative officials.

-Ensure servers are protected in rooms watched 24/7 be a security official and cameras that detect unauthorised movement/access in the room and notifies all security officials in the building. The room is then securely ventilated and cooled, with strong stable doors (metal) with security code requirements that include: a guard that checks the identification of officials who will then proceed to the final security measure of a biometric retina scan.

-If IT/Administrator wants to access server the server must first be protected with a 16 Character password with at least one capital, lower, and special character and identification number along with retina scan at their computer location within Global Telecommunications facility.

-Educate those to not share information with others, not even to fellow peers. If so direct them to a Data Monitoring Committee official if the password has been forgotten.

-**The Data Monitoring Committee** (whom are IT/Administrative officials) must establish acceptable levels of security risk for resources by assessing factors such as:

-Ensure that the server and every account in the server password is reset every 30 days. The passwords are automatically reset. User will have to receive new password after passing identity security protocols, which include presentation of identification, name and date of birth. The employee/official information should be simple and easy to find by creating an effective data classification app with an algorithm that safely and effectively receives data within the server.

-Locating where your sensitive data resides within the organization.

-Since all data is sensitive, ensure that company provided flash drives (and other portable storage devices) are encrypted and have anti-virus implemented in them. In the event that highly important hard drives are to be transported to another location. The storage should be storage in a air-tight, water and fireproof space that inhibits outside signals. The case should then be handcuffed to a security official protected by other armed security officials.

-Access Global Telecommunications Cloud Data Centers must require permission from a data security official and must pass the security test which includes proof of their work/private identification, data of birth, etc. The persons and changes that are outside of their privilege should require further security test from officials.

-In the event that there is a power outage of a natural disaster that threatens the servers, the backup generator automatic power on to ensure that data is restored automatically while running a diagnostic and security test on all of the data in rest in the building to ensure that everything is running smoothly and secure.

-Employing data encryption to multiple locations and cover structured and unstructured data.

-Realizing that the value of data changes over time and new data will require an immediate plan, while certain archived data may no longer pose a security risk. (The University Policy Manual)

-The level of criticality or overall importance to the continuing operation of the campus as a whole, individual departments, research projects, or other essential activities; (The University Policy Manual)

-While still considering the overall security of the Global Telecommunications, asses how negatively the operations of one or more units would be affected by unavailability or reduced availability of the resources by monitoring all data. (The University Policy Manual)

-How likely it is that a resource (both data in rest and motion)could be used as a platform for inappropriate acts towards other entities. (The University Policy Manual)

-Limits of available technology, programmatic needs, cost, and staff support; (The University Policy Manual)

-Ensure that each employee and official gets a company computer and phone that has an application that monitors and encrypts all that is relayed and received. The application actively classifies whether the information the employee creates or receives is threatening to Global Telecommunications and immediately notifies a 24/7 monitor official and/or data monitor committee official on call.

-Emails are monitored 24/7 by an assigned data monitoring committee officials along with a learning algorithm that inhibits certains actions and access of the user if a threat is foreseen.

**Providers** (individuals who design, manage, and operate campus electronic information resources, e.g. project managers, system designers, application programmers, or system administrators) must follow the same rules that apply to them stated in the rules for IT/Administrative officials along with:

* Becoming knowledgeable regarding relevant security requirements and guidelines;
* Analyzing potential threats and the feasibility of various security measures in order to provide recommendations to Administrative Officials;
* Implementing security measures that mitigate threats, consistent with the level of acceptable risk established by administrative officials; (The University Policy Manual)
* Establishing procedures to ensure that privileged accounts are kept to a minimum and that privileged users comply with their access agreements/restrictions.

**Users** (individuals who access and use campus electronic information resources) must knowledgeable of the rules of the IT/Administrators and Providers along with:

* Becoming knowledgeable about relevant security requirements and guidelines. (The University Policy Manual)
* Protect the resources under their control, such as access passwords, computers, data they download on their company devices.
* Know that outside devices not provided by the company must be left at home or has to go through a through security check from the Data Monitoring Committee each entry into the premise.
* Never share passwords or devices with others including workplace peers.
* Ensure that the device your insert your portable device into is secure by going over the guidelines provided by Providers and IT/Administrative Officials.

Reference

Campus Information Technology Security Policy. (2016). Retrieved August 22, 2016,

from <https://security.berkeley.edu/campus-information-technology-security-policy>

<https://www.sophos.com/en-us/medialibrary/PDFs/other/sophos-example-data-security-policies-na.pdf?la=en>

The University Policy Manual. (2016). Retrieved August 22, 2016, from

<https://policy.uncg.edu/university-policies/data/>

Secure The Breach | Get Ready For A Security Breach. (n.d.). Retrieved August 30,

2016, from <http://www.securethebreach.com/encryption.html>

Information Security | Washington University in St. Louis. (2016). Retrieved August 22,

2016, from https://wustl.edu/about/compliance-policies/computers-internet-policies/information-security/