Water Treatment Physical Security Policy

Matthew Austin

Fontbonne University

Quagliata

November 2016

**Water Treatment Physical Security Policy**

*Using this policy*

This policy defines the physical security policy for data and safety within organization to ensure protection of such data and the staff within.

*Scope*

This policy applies to all equipment and data owned and operated by the organization and to all staff members regardless of the environment where the data and staff members reside. The policy applies regardless of the media or department on which the employee or data reside or the form that it may take.

*Definitions*

**Biometrics:** The application of statistical analysis to biological data.

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

**Physical Security:** Security of staff members that are working the organization. Physical security also entails protecting the data of the staff to ensure the information is not used to physically harm them.

***Roles & Definitions***

The facilities responsibilities of the the assets and physical security staff 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 owned or associated and staff that are employed with our organization.

*Policy*

**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 organization 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 weather safe rooms (such as water, fire, etc.) watched 24/7 be a security officials and cameras that detect unauthorised movement/access in the room and notifies all security officials in the building. The security of the servers and information of staff is important. If the information is under threat there is a chance that the information will be used to harm our employees and our facility. Within the server rooms there are security officials on duty watching the facility to ensure not only the safety of our employees thought the multitude of cameras that are installed throughout the facility, but to also prevent unwarranted entries. 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 to the room and the server must they 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. Employees should also be aware of their surroundings to that they won't be tailgated to prevent threats to not only the afilicty but to those who use our services. 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 (through data and through camera security) 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.

-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.

-Realizing that the value of the assets within the organization does change over time and new security details 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 those on campus as a whole, individual departments, research projects, etcs.

-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 and employees through the camera security system. (The University Policy Manual)

-How likely it is that a resource (both data and employees physical security)could be used as a platform for inappropriate acts towards other entities.

-Limits of available technology, programmatic needs, cost, and staff support

-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. Employees will also have to be accompanied by a device that checks their heart rate to to asses if they are in danger. The device also is equipped with a button that sends a signal that details their location 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, in this case any threat to an employee is a threat to the physical security of employees and the workflow of the our water treatment plant which is crucial.

**Providers** (individuals who design, manage, and operate organization 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, Again the information that is protected, is for the physical safety of the employees.

* 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;)
* Establishing procedures to ensure that privileged accounts are kept to a minimum and that privileged users comply with their access agreements/restrictions.

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

* Becoming knowledgeable about relevant security requirements and guidelines.
* 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/