Unit 10 Full Policy Drafting

**Corey Crooks**

**Purdue University Global**

**IT484—Cybersecurity Policies**

**Preston Rich**

**February 21, 2023**

Cybersecurity policies dictate how exactly an organization goes about their daily functions and the restrictions that are imposed in the individuals that operate within the organization and its boundaries. Because of this, proper documentation is to be upheld regarding the security policy at all times should a breach event occur, and the organizational data that are within be compromised. In the event of a disaster organizational resources such as security policies must be produced in an efficient manner to ensure that employees interacting with the organization during such an event may have a clean, and organized manner in which they are able to respond to the event with the efficiency utilize (Brown University Office of Information Technology, 2021). This will in turn protect both the organization, and those clients that it interacts with to provide a more stable and rewarding business opportunity for everyone involved. To upkeep this tradition and ensure proper logistical maintenance regarding security concerns, a broad security portfolio is required to be developed in the initial stages of a security firm, or technological business. It is extremely important that a business develop these logistical plans and strategies at the start of their business should employees have questions regarding when disaster strikes (SANS Institute, 2022). These questions may turn into more elaborate and costly confusion during the time of an event, and could have been remedied earlier on via proper documentation. Due to this, knowledge on policy platforms regarding the organization that one interacts with is paramount to the success of the organization itself.

The following is a full cyber security policy with regards to a scenario that an organization is gathering resources to develop a cloud storage platform. This cloud storage platform would utilize clients that require large volume of storage off of their initial sites of contact. This organization would then host external organizations data within their internal storage platforms.

Documentational Policies

* All employees of the organization are two sine standard policy agreements. These agreements cover the content of these policy drafts, and ensure understanding of all information contained within.
* Employees of the organization Shell also have a copy of policies that they sign within their personal retrieval.
  + Storage of these policies is up to the individual employee but must be relevant to organizational security. For example, policies can be stored in print on paper within an employee’s desk, or digitally within an employee’s email inbox. An employee should be able to retrieve these policies at a moment’s notice whenever required.
  + The human resources branch of this organization will be the required correspondence for these policies. Human resources will oversee that each employee new or existing winner policy gets drafted, or when an employee is hired shall receive a copy of relevant policies that they may overlook as they require.
  + Human resources will serve as the field for questions and analysis of employees that need to ask any clarifying questions regarding the policies that they are expected to uphold. Human resources will be required to help employees understand exactly how the employees with questions are able to get in touch with those that could produce reasonable answers to their questions regarding organizational policies.

Policy Compliance

* To ensure and aid in policy compliance mandatory learning sessions should be scheduled with those that interact with critical functions in the organization. These learning sessions should involve critical functions that the employee oversees, as to be relevant to their daily job functions.
  + It is also important that all organizational employees are subjected to training resources and lessons regarding best behavior and practices there within for common unintended malicious behavioral mechanisms to be remedied in the meeting, or shortly thereafter. This meeting will cover basic network activities, and warning signs for malicious actors to be cognizant of in order to mitigate the chances of a security breach due to improper behavior. Key concepts for these learning functions to cover would be behavioral techniques to mitigate the spread of confidential information, and warning signs for phishing scams.

Acceptable Use (Brown University Office of Information Technology, 2021)

* Employees are under no circumstances allowed to view or access client information without the necessary exemptions from a chief security officer. Accessing confidential client information may result in the termination of an employee’s status with the organization pending an investigation from the chief security officer, and authorized staff.
* Employees under no circumstances are allowed to modify client information via internal or external tools. Circumstances such as informational validity targeted from an employee or an automated system that an employee oversees may result in the termination of said employee pending an investigation from the chief security officer, and authorized staff.
* The introduction of intentional or unintentional malicious activity, or programs into the organizations network, or any network they commonly interacted with may result in the termination of an employee’s status with the organization pending an investigation from the chief security officer, and authorized staff.
* Employees, or those the organization interacts with, shall not share sensitive information regarding the organization or its concepts via any external means. This involves sharing job functions and confidential information on public forums such as social media.
  + Employees are not to communicate on public forums regarding information that the organization may hold in some form of secrecy. Employees will not share information via any means that may provide a risk to the organization, and those that interact with.
  + Should an employee share confidential information via external means that may provide a risk to the organization in those that interacts with, they will be subjected to a meeting with the chief security officer to discuss behavioral alterations. If this was not the first meeting with the chief security officer, they may also discuss termination of the employee’s status with the organization.

IT Security for Risk Assessment (The National Institute of Standards and Technology, 2024)

1. Security Categorization

The IT Department will be upheld to:

* Maintain security controls on physical and digital levels for confidential data as designated by system owners and executive personnel.
* Document security controls both physical and digital in a security plan to be reviewed by associated stakeholders with security control rationale and use-case.

1. Risk Assessment

The IT Department will be upheld to:

* Oversee or conduct a proper assessment of risk from logical factors malicious or otherwise related to proper use-cases of the organization and their materials.
* Document the Risk Assessment and the findings annually in respective organization.
* Review Risk Assessment findings with associated executive stakeholder’s minimum once per quarter, or when new potential security risks become known; whichever is soonest.
* Update the Risk Assessment regularly with new factors and disciplines that could impact the organization’s well-being.

1. Vulnerability Scanning

The IT Department will be upheld to:

* Employ vulnerability scanning tools and techniques to identify key factors such as software flaws, mis-aligned configurations, and back-end design philosophies that may provide additional vulnerabilities to the organization and its assets.
  + This scan should be done quarterly with documentation on the temporal data, and findings recorded to be reviewed by executive stakeholders.
* Report results of the vulnerability scan to associated executive stakeholders, and answer clarification information with insights and automation no less than 31 days after each scan is done.
* Action upon threatening vulnerabilities within 31 days of the stakeholder briefing.
* Employ regular system updates to handle security vulnerabilities that are highlighted in such briefings.
* Ensure security controls are upheld at each stage in the vulnerability scan, and that controls remain active throughout the lifetime of the organization.

Access Controls

1. Employee training
   1. Employees will undergo a series of informational lectures regarding security policies that focus on physical security and behavioral mechanisms to maintain physical security.
   2. Employees will have a direct route to training personnel that they may use to ask questions, or gather further information relating to physical security policies being implemented in the organization.
2. Access Cards
   1. Physical cards are to be kept on all related security personnel at all times during their daily job functions.
   2. Physical Cards will not be switched between personnel under any circumstances.
   3. Compromised cards that have been lost, or are suspected to be cloned will be reported no later than one day after it comes to the attention of staff.
      1. These cards will be replaced using a new set of identity metrics at the discretion of the Chief Security Officer.
      2. The Employee responsible for the maintenance of their card will be recorded.
         1. If there have been no other security concerns related to this employee, they will be instructed to attend a mandatory security meeting to enforce compliance through understanding.
         2. If there have been one or two security breach events regarding this employee, they will receive written notice and be scheduled a meeting with supervisors to discuss behavioral adaptations.
         3. If there have been three or more security events regarding this employee, their employment with the organization will be terminated.
3. Physical Locks and Critical Entry Points
   1. Locks will be placed on all entry points to critical systems and data centers.
      1. These locks will respond and open upon presentation of a valid access card by organization staff.
      2. These locks will allow for automatic shutdown in cases of emergency to refuse entry to any personnel regardless of access card clearance.
      3. These entry points will have an automatic opening located within the data center to allow for personnel to escape in the event of a disaster such as a fire within the critical system.
         1. These automatic opening switches are not to be accessible by any means from the outside areas.
   2. Locks will utilize asymmetric encryption platforms with PGP integration with checking privilege information to ensure relevant and accurate entry information to prevent recently terminated employees or compromised cards from entry.

Exemption

* No employee or contact of the organization is to be considered exempt on any default basis. In order for an employee to become exempt to any tenants list listed above, they must first apply with the chief security officer in order to detail the methods, and reason of their exemption. This letter will also detail the specific tenants they believe they should be exempt from as well as a summary of risks posed by a non exemption from these tenants.
  + The chief security officer will then review this exemption request, and deliver their bases within three business days.

Employee Approval

* An employee is expected to sign each policy that they would reasonably need to uphold. This signature verifies understanding of the policy, and provides for a commitment of good faith to uphold the policy in all reasonable accounts.
  + Should an employee sign these policies, and willingly fail to uphold them during their daily job functions they will be subjected to a meeting with the chief security officer to discuss either behavioral changes to their conduct in the office, or termination of the employee’s status within the organization.

Cybersecurity policies are imperative for the lifetime of an organization, and the secure operation of both the organization and those that interacts with. Due to this imperative nature, the full policy is expected to be known by employees of the organization and to be acted upon with respect and commitment throughout an employee’s daily job functions (SANS Institute, 2022). Failing that, the employee will be met with appropriate consequence to correct this behavior in the future. Terminations with the first offense of an incident is an impractical business strategy, and thus transparency and meetings are to be provided and maintained as the first point of consequence for most any security risk posed by an internal threat (Human Resources of the University of Nebraska Omaha, n.d.). During these transparency meetings, employees should be focused on maintaining best practice behavior and posing questions to understand further why exactly these policies are put in place, and how they can help the employee in their daily job functions to be more secure about their interaction with their environment around them. As transparency is key in this exchange employees are encouraged to ask questions throughout their employment with the organization in order to better understand both the facilities that it employs and the strategy that it adopts in order to run a more secure environment for all those that it oversees.

# **References**

Brown University Office of Information Technology. (2021, July 18). *Acceptable Use of Information Technology Resources Policy*. Retrieved from Brown University Policies: https://policy.brown.edu/policy/acceptable-use-it-resources

Human Resources of the University of Nebraska Omaha. (n.d.). *Disciplinary Action Steps for the Written Warning*. Retrieved from unomaha: https://www.unomaha.edu/human-resources/employee-relations-and-staff-development/steps-for-the-written-warning.php

SANS Institute. (2022, October). *Acceptable Use*. Retrieved from Security Policy Template: https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/blt207beda4b7c14d22/636f1a30e3836b0c88e8f0a8/Acceptable\_Use\_Policy.pdf

SANS Institute. (2022, October). *Communications Equipment Policy*. Retrieved from Consensus Policy Resource Community: https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/blta17c9161050b163c/5e9e02845352ae2926038860/communications\_equipment\_policy.pdf

The National Institute of Standards and Technology. (2024, February 17). *Policy Template Guide*. Retrieved from The NIST Cybersecurity Framework: https://www.cisecurity.org/-/jssmedia/Project/cisecurity/cisecurity/data/media/img/uploads/2021/11/NIST-Cybersecurity-Framework-Policy-Template-Guide-v2111Online.pdf