SNOWBE ONLINE

Security Maturity Policy

Your name: Pedro Portillo

Security Maturity Policy

DATE: 9/1/2024

Security Maturity Policy
Status: ☒ Working Draft ☐ Approved ☐ Adopted
Document owner: Pedro Portillo
DATE: 9/1/2024

Table of Contents

Purpose

This Information Security Plan outlines SnowBe’s ongoing efforts to secure information related to students and other stakeholders who provide sensitive information to the University. The University is required by federal law, specifically the Gramm-Leach Bliley Act, to implement safeguards to protect non-public personal data, information, and resources. These safeguards are provided to:

- Make reasonable efforts to ensure the security and confidentiality of sensitive data, information, and resources.

- Protect against anticipated threats or hazards to the security or integrity of such information; and

- Protect against unauthorized access to or use of confidential data, information, and resources that could result in substantial harm or inconvenience to any consumer.

Howard University adopted the following Information Security Plan as a measure to protect the confidentiality, integrity, and availability of institutional data as well as any Information Technology (IT) assets. This plan provides for mechanisms to:

- Identify and assess the risks that may threaten sensitive data, information, and resources maintained by the company.

- Manage and control these risks.

- Implement and review the plan; and

- Adjust the plan to reflect changes in technology, the sensitivity of confidential data, information and resources, and internal or external threats to Information Security.

Scope

This plan applies to all students, faculty, staff, and third-party agents of Howard University as well as any other University affiliate who is authorized to access the University’s data and IT resources.

Definitions

Confidentiality: Protection of information from unauthorized access or disclosure.

Data Custodian: An employee responsible for the administrative and operational management of Institutional Data.

Data Steward: An employee responsible for overseeing the lifecycle and classification of Institutional Data.

Information Security Plan: A strategic approach to protect sensitive data, information, and resources.

Integrity: Assurance that information is accurate and reliable.

Institutional Data: Data classified as public, private, or restricted based on its sensitivity and value.

Risk Management: The process of identifying, assessing, and controlling threats to an organization's information.

Security Breach: An incident that results in unauthorized access to data or information.

Security Controls: Measures implemented to safeguard data and information systems.

User: Any individual authorized to access Institutional Data or Information Systems.

Roles & Responsibilities

Howard University's Information Security Plan states that "Individuals who are authorized to access Institutional Data shall adhere to the appropriate Roles and Responsibilities, as defined in documentation approved by the Howard University Policy Committee, and maintained by the Information Security Office." These roles and responsibilities are defined as follows:

3.1 University Policy Committee

The Howard University Policy Committee (UPC) manages a coordinated, enterprisewide policy process that supports the University and its mission. The UPC facilitates effective decision-making, promotes effective control over business process and flow, and prevents institutional exposure through a transparent, uniform, and inclusive policy management process by:

- Reviewing and recommending strategies to implement the Information Security Plan.
- Analyzing the business impact of proposed strategies on the University.
- Approving proposed strategies. 4
- Serving as a champion for accepted strategies within respective business units and/or colleges.
- Overseeing the review and approval of Information Security Plan exceptions.

3.2 Director of Information Security

The Director of Information Security is a senior-level employee of the University who oversees the University's Information Security Program. Responsibilities of the Director of Information Security include the following:

a. Developing and implementing a company-wide Information Security Program.
b. Documenting and disseminating Information Security policies and procedures.
c. Coordinating the development and implementation of a Universitywide Information Security Training and Awareness Program.
d. Coordinating a response to actual or suspected breaches in the confidentiality, integrity, or availability of Institutional Data.

3.3 Data Steward

A Data Steward is an employee of the University who oversees the lifecycle of one or more sets of Institutional Data. Responsibilities of a Data Steward include the following:

a. Assigning an appropriate classification to Institutional Data.

All Institutional Data should be classified based on its sensitivity, value, and criticality to the University. The University has adopted three primary data classifications: public, private, and restricted. See Appendix A Guidelines for Data Classification for more information.

b. Assigning day-to-day administrative and operational responsibilities for Institutional Data to one or more Data Custodians.

Data Stewards may assign administrative and operational responsibility to specific employees or groups of employees. A Data Steward could also serve as a Data Custodian. In some situations, multiple groups will share Data Custodian responsibilities. If multiple groups share responsibilities, the Data Steward should understand which group performs which functions.

c. Approving standards and procedures related to day-to-day administrative and operational management of Institutional Data.

While it is the responsibility of the Data Custodian to develop and implement operational procedures, it is the Data Steward's responsibility to review and approve these standards and procedures. A Data Steward should consider the classification of the data and associated risk tolerance when reviewing and approving these standards and procedures. For example, high-risk and/or highly sensitive data may warrant more comprehensive documentation and, similarly, a more formal review and approval process. A Data Steward should also consider his or her relationship with the Data Custodian(s). For example, different review and approval processes may be appropriate based on the reporting relationship of 5 the Data Custodian(s).

d. Determining the appropriate criteria for obtaining access to Institutional Data. A Data Steward is accountable for who has access to Institutional Data.

This does not imply that a Data Steward is responsible for day-to-day provisioning of access. Provisioning access is the responsibility of a Data Custodian. A Data Steward may decide to review and authorize each access request individually, or a Data Steward may define a set of rules that determine who is eligible for access based on business function, support role, etc. For example, a simple rule may be that all students are permitted access to their transcripts or all staff members are permitted access to their own health benefits information. A Data Custodian should document these rules in a manner that allows little or no room for interpretation.

e. Ensuring that Data Custodians implement reasonable and appropriate security controls to protect the confidentiality, integrity, and availability of Institutional Data.

The Information Security Office has published guidance on implementing reasonable and appropriate security controls based on three classifications of data: public, private, and restricted. See Appendix A Guidelines for Data Classification for more information. Data Stewards will often have their security requirements specified in contractual language and/or based on various industry standards. Data Stewards should be familiar with their unique requirements and ensure Data Custodians are also aware of and can demonstrate compliance with these requirements. The Information Security Office can assist with mapping controls identified in guidelines for data protection to controls mandated by contract(s) or industry standards.

f. Understanding and approving how Institutional Data is stored, processed, and transmitted by the University and by third-party agents of the University.

To ensure reasonable and appropriate security controls are implemented, a Data Steward must understand how data is stored, processed, and transmitted. This can be accomplished through a review of data flow documentation maintained by a Data Custodian. In situations where Institutional Data is being managed by a third party, the contract or service level agreement should require documentation of how data is or will be stored, processed, and transmitted.

g. Defining risk tolerance and accepting or rejecting risk related to security threats that impact the confidentiality, integrity, and availability of Institutional Data.

Information Security requires a balance between security, usability, and available resources. Risk Management plays an important role in establishing this 6 balance. Understanding what classifications of data are being stored, processed, and transmitted will allow Data Stewards to better assess risks. Understanding legal obligations and the cost of non-compliance will also play a role in this decision-making. Both the Information Security Office and the Office of General Counsel can assist Data Stewards in understanding risks and weighing options related to data protection.

h. Understanding how Institutional Data is governed by University policies, state and federal regulations, contracts, and other legally binding agreements.

Data Stewards should understand whether or not any University policies govern their Institutional Data. For example, the Information Security Policy governs the protection of all Institutional Data. The Policy on Student Privacy Rights specifically addresses the privacy of student information. Other policies exist to help govern financial information, health information, etc. Visit Howard University’s policy website (https://www.howard.edu/secretary/policy/) for a comprehensive list of University policies. Similarly, Data Stewards are responsible for having a general understanding of legal and contractual obligations surrounding Institutional Data. For example, the Family Educational Rights and Privacy Act (FERPA) dictates requirements related to the handling of student information. The Office of General Counsel can assist Data Stewards in gaining a better understanding of legal obligations.

3.4 Data Custodian

A Data Custodian is an employee of the University who has administrative and/or operational responsibility over Institutional Data. In many cases, there will be multiple Data Custodians. An enterprise application may have teams of Data Custodians, each responsible for varying functions. A Data Custodian is responsible for the following:

a. Understanding and reporting on how Institutional Data is stored, processed, and transmitted by the University and by third-party agents of the University.

Understanding and documenting how Institutional Data is being stored, processed, and transmitted is the first step toward safeguarding that data. Without this knowledge, it is difficult to implement or validate safeguards effectively. One method of performing this assessment is to create a data flow diagram for a subset of data that illustrates the system(s) storing the data, how the data is being processed, and how the data traverses the network. Data flow diagrams can also illustrate security controls as they are implemented. Regardless of approach, documentation should exist and be made available to the appropriate Data Steward.

b. Implementing appropriate physical and technical safeguards to protect the confidentiality, integrity, and availability of Institutional Data.

The Information Security Office has published guidance on implementing 7 reasonable and appropriate security controls for three classifications of data: public, private, and restricted. See the Guidelines for Data Classification and the Guidelines for Data Protection for more information. Contractual obligations, regulatory requirements, and industry standards also play an important role in implementing appropriate safeguards. Data Custodians should work with Data Stewards to gain a better understanding of these requirements. Data Custodians should also document what security controls have been implemented and where gaps exist in current controls. This documentation should be made available to the appropriate Data Steward.

c. Documenting and disseminating administrative and operational procedures to ensure consistent storage, processing, and transmission of Institutional Data.

Documenting administrative and operational procedures goes hand-in-hand with understanding how data is stored, processed, and transmitted. Data Custodians should document as many repeatable processes as possible. This will help ensure that Institutional Data is handled consistently. This will also help ensure that safeguards are being effectively leveraged.

d. Provisioning and de-provisioning access to Institutional Data as authorized by the Data Steward.

Data Custodians are responsible for provisioning and de-provisioning access based on criteria established by the appropriate Data Steward. As specified above, standard procedures for provisioning and de-provisioning access should be documented and made available to the appropriate Data Steward.

e. Understanding and reporting on security risks and how they impact the confidentiality, integrity, and availability of Institutional Data.

Data Custodians should have a thorough understanding of security risks impacting their Institutional Data. For example, storing or transmitting sensitive data in an unencrypted form is a security risk. Protecting access to data using a weak password and/or not patching a vulnerability in a system or application are both examples of security risks. Security risks should be documented and reviewed with the appropriate Data Steward so that he or she can determine whether greater resources need to be devoted to mitigating these risks. The

Information Security Office can assist Data Custodians with gaining a better understanding of their security risks.

3.5 User

For information security, a User is any student, employee, contractor, or third-party agent of Howard University who is authorized to access University Information Systems and/or Institutional Data. A User is responsible for the following:

a. Adhering to policies, guidelines, and procedures about the protection of Institutional Data.

   The Information Security Office publishes various policies, guidelines, and procedures related to the protection of Institutional Data and Information Systems. They can be found on the ETS website under Information Security. Business units and/or Data Stewards may also publish their unique guidelines and procedures. Information on requirements unique to your business unit or a system you have access to can be found by talking to your manager or system administrator.

b. Reporting actual or suspected vulnerabilities in the confidentiality, integrity, or availability of Institutional Data to a manager or the Information Security Office.

   During day-to-day operations, if a User comes across a situation where he or she feels the security of Institutional Data might be at risk, it should be reported to the Information Security Office. For example, if a User comes across sensitive information on a website that he or she feels shouldn’t be accessible, that situation should be reported to the Information Security Office. Additional notifications may be appropriate based on procedures unique to a business unit or defined by a Data Steward. It may be appropriate to notify a local security point of contact that will in turn coordinate with the Information Security Office.

c. Reporting actual or suspected breaches in the confidentiality, integrity, or availability of Institutional Data to the Information Security Office.

   Reporting a security breach goes hand-in-hand with reporting vulnerabilities. Once again, it may be appropriate to notify a local security point of contact that will in turn coordinate with the Information Security Office.

Project Manager:

- Oversees the entire SDLC process, ensuring the project stays on track, within budget, and meets requirements.

- Coordinates communication among all stakeholders and manages risks.

System Architect:

- Designs the overall system structure and ensures it aligns with business and security requirements.

- Provides technical oversight throughout the SDLC.

Development Team:

- Develops, tests, and debugs the system according to specifications.
- Ensures code quality and security are maintained.

Quality Assurance (QA):

- Develops and executes testing plans to ensure the system functions as intended.
- Identifies and helps resolve defects.

Security Officer:

- Integrates security controls into all phases of the SDLC.
- Conducts security assessments and ensures compliance with policies.

Operations Team:

- Manages system deployment and ongoing maintenance.
- Monitors system performance and handles updates and troubleshooting.

Policy

Throughout its lifecycle, all Institutional Data shall be protected in a manner that is considered reasonable and appropriate, as defined in documentation approved by the Howard University Policy Committee and maintained by the Information Security Office, given the level of sensitivity, value, and criticality that the Institutional Data has to the University.

Any Information System that stores, processes, or transmits Institutional Data shall be secured in a manner that is considered reasonable and appropriate, as defined in documentation approved by the Howard University Policy Committee and maintained by the Information Security Office, given the level of sensitivity, value, and criticality that the Institutional Data has to the University.

Individuals who are authorized to access Institutional Data shall adhere to the appropriate Roles and Responsibilities, as defined in documentation approved by the Howard University Policy Committee and maintained by the Information Security Office.

Exceptions/Exemptions

SnowBe Online mandates that any part of its Security Plan that does not meet compliance criteria be requested as an exemption by staff members, vendors, or contractors. Requests for exceptions must be approved by the Chief Information Security Officer and the appropriate Unit Head after taking risks and mitigating circumstances into account. The ISO assesses exceptions, approving them temporarily for a maximum of a year before reevaluating them every year for possible renewal. Elements of the Security Plan that are not compliant may be subject to removal or remedial action. Requests may be forwarded to the CISO for consideration if they are denied or have expired.

SnowBe Online allows exemptions for any aspect of its Security Plan that requires alternative controls, subject to written approval by the CISO and relevant Unit Head. Exemptions are granted for a maximum of one year and must be reviewed annually. Non-compliant elements of the Security Plan may be subject to corrective actions or removal. If unapproved or expired, the matter is escalated to the CISO, who coordinates with IT and functional stakeholders.

Enforcement

SUIT is responsible for managing security assessments for SnowBe according to established requirements authorized in the SUIT Security Program Policy. Any systems under the policy authority of SUIT with requirements that deviate from the SUIT Security Program policies are required to submit a Policy Exemption Form to SUIT for consideration and potential approval. Any attempt by personnel to circumvent or otherwise bypass this policy or any supporting policy will be treated as a security violation and subject to investigation. The results of the investigation may entail written reprimand, suspension, termination, and possibly criminal and/or civil penalties.

Citations

Howard University. (n.d.). *Information security plan*. Retrieved from https://technology.howard.edu/sites/technology.howard.edu/files/2020-03/Information_Security_Plan_0.pdf