HOWARD UNIVERSITY INFORMATION SECURITY PLAN

Jonathan F. Piersol
Associate Vice President & Chief Information Officer

Revised November 1, 2019

Table of Contents

Document Control Table

Version	Date	Author	Rationale
1.0	January 2014	Christopher Cole	Original Draft
2.0	August 2014	Christopher Smith	Final Revision
3.0	November 2019	Oreoluwa Onatemowo	Review/Revision

1. Introduction

1.1 Purpose

This Information Security Plan outlines Howard University'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 University;
- 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.

1.2 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.

1.3 Maintenance

This plan will be reviewed by the University's Information Security Office annually or as deemed appropriate based on changes in technology or regulatory requirements.

1.4 Enforcement

Violations of this plan may result in suspension or loss of the violator's use privileges, with respect to Institutional Data and University-owned Information Systems. Additional administrative sanctions may apply; up to and including termination of employment or contractor status with the University, or expulsion of student workers. Civil, criminal and equitable remedies may also apply.

1.5 Exceptions

Exceptions to this plan must be approved by the Information Security Office, under the guidance of the University's Chief Information Officer and Executive Vice President and Chief Operations Officer. All exceptions will be formally documented. Plan exceptions will be reviewed on a periodic basis for appropriateness.

2. Policies

2.1 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.

2.2 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.

2.3 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.

3. Roles and 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, enterprise-wide 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:

a. Reviewing and recommending strategies to implement the Information Security Plan.
b. Analyzing the business impact of proposed strategies on the University.
c. Approving proposed strategies.

d. Serving as a champion for accepted strategies within respective business units and/or colleges.
e. 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 University-wide Information Security Program.
b. Documenting and disseminating Information Security policies and procedures.
c. Coordinating the development and implementation of a University-wide 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

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 own 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 own security requirements specified in contractual language and/or based on various industry standards. Data Stewards should be familiar with their own 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.

In order 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 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

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 legal 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 in an effective manner. 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

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 in a consistent manner. 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 the purpose of 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 pertaining to 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 own 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 the course of 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.

4. Design and Implementation of Safeguards Program

4.1 Employee Management and Training

Employees in departments that use or have access to non-public data in the course of their work for the University receive training on the importance of the confidentiality of sensitive information, including a review of the requirements of federal laws. Employees are trained in how to avoid risks such as mobile device theft, wireless snooping, phishing attacks, virus infections and spyware. Employees are also trained in the importance of keeping passwords secure. Departments which routinely handle sensitive data are responsible for training their employees in controls and procedures to prevent employees from providing confidential information to unauthorized individuals. Employees are also trained how to properly dispose of documents that contain personal information. Each department responsible for maintaining student and employee personal information is instructed to take steps to protect the information from destruction, loss or damage due to environmental hazards, such as fire and water damage or technical failures. These training efforts help to minimize risk and safeguard Information Security.

4.2 Physical Security

Howard University has addressed the physical security of non-public sensitive data by limiting access to only those employees who have a business reason to know such information. Non-public data is available only to University employees with an appropriate business need for such information.

Paper documents containing sensitive information are kept in locked office file cabinets or rooms. Only authorized employees have access to those spaces. Storage areas holding paper documents containing non-public information are kept secure at all times. No paper documents containing sensitive information may be removed from campus. Paper documents that contain personal, non-public information are shredded or securely destroyed at the time of disposal.

4.3 Information Systems

Access to data via the University's computer information systems is limited to individuals who have a business reason to know such information. Each employee is assigned a username and password, and multi-factor authentication is required. Databases containing non-public data, including but not limited to accounts, balances and transactional information, are available only to University employees in appropriate related departments and positions.

Enterprise Technology Services (ETS) takes reasonable and appropriate steps consistent with current technological developments to make sure that all data in electronic form is secure and to safeguard the integrity of records in storage and during transmission. ETS runs threat detection software to identify systems that are compromised and/or infected so they can take appropriate steps to mitigate the risk. Passwords for central software systems are required to comply with complexity rules and must be changed regularly. When technically feasible, encryption technology is utilized for transmission of sensitive data. All non-public data stored on laptops or other portable devices must be encrypted. When personal computers are redeployed, all memory components are completely reformatted or otherwise erased for any new use.

4.4 Responding to System Failures

Howard University maintains systems to prevent, detect and respond to attacks, intrusions and other system failures. ETS regularly reviews network access and security policies and procedures, as well as protocols for responding to network attacks and intrusions. Any security breaches or other system failures must be reported immediately to the Information Security Office. Office personnel are responsible for documenting responsive actions taken in connection with any incident involving a breach of security, and mandatory post-incident review of events and actions taken, if any, to make changes in business practices relating to protection of information.

5. Service Provider Oversight

Whenever the University retains a service provider that will maintain, process or have access to student or employee information, the University will ensure that the provider has in place an information security program sufficient to protect sensitive data. The University will include in the contracts with service providers having access to non-public information a provision requiring the providers to have in place security measures consistent with the requirements of federal regulations and to assure that such information is used only for the purposes set forth in the contract.

6. Computer System Security Infrastructure

Howard University maintains a computer security system that provides:

a. Secure user authentication protocols including:

- control of user IDs and other identifiers;
- a secure method of assigning and selecting passwords;
- control of data security passwords to ensure that such passwords are kept in a location and/or format that does not compromise the security of the data they protect;
- restricting access to active users and active user accounts only; and
- blocking access to user identification after multiple unsuccessful attempts to gain access or the limitation placed on access for the particular system.

b. Secure access control measures that:

- restrict access to records and files containing sensitive information to those who need such information to perform their job duties; and
- assign unique identifications plus passwords, which are not vendor supplied default passwords, to each person with computer access, that are reasonably designed to maintain the integrity of the security of the access controls.

c. Encryption of all transmitted records and files containing non-public information that will travel across public networks, and encryption of all data containing personal information to be transmitted wirelessly.

d. Monitoring of systems, for unauthorized use of or access to non-public information.

e. Encryption of all personal information stored on laptops or other portable devices.

f. For files containing sensitive information on a system that is connected to the Internet, there must be up-to-date firewall protection and operating system security patches, designed to maintain the integrity of the information.

g. Up-to-date versions of system security agent software which must include malware protection and up-to-date patches and virus definitions, or a version of such software that can still be supported with up-to-date patches and virus definitions, and is set to receive the most current security updates on a regular basis.

h. Education and training of employees on the proper use of the computer security system and the importance of non-public information security.

Information Security Office personnel work with the appropriate University departments to ensure that this security system infrastructure is appropriately maintained.

7. Retention of Sensitive Information

Sensitive, non-public information will only be retained for as long as needed for the University's reasonable business purposes, including for the purpose of complying with any local or federal law. Each department that stores such information will annually review the non-public data it has retained for the purpose of determining which information may be purged.

8. Termination of Access to Sensitive Data

Once an employee who has access to sensitive data concludes his/her employment, either voluntarily or involuntarily, such employee's access to said data shall be terminated.

9. Appendix A – Data Classification

9.1 Purpose

The purpose of these guidelines is to establish a framework for classifying Howard University's data based on its level of sensitivity, value and criticality to the University as required by Howard University's Information Security Plan. Classification of data will aid in determining baseline security controls for the protection of data.

9.2 Data Classification

Data classification, in the context of Information Security, is the classification of data based on its level of sensitivity and the impact to the University should that data be disclosed, altered or destroyed without authorization. The classification of data helps determine what baseline security controls are appropriate for safeguarding that data. All Institutional Data should be classified into one of three sensitivity levels, or classifications:

A. Restricted Data

Data should be classified as **Restricted** when the unauthorized disclosure, alteration or destruction of that data could cause a significant level of risk to the University or its affiliates. Examples of Restricted data include data protected by state or federal privacy regulations and data protected by confidentiality agreements. The highest level of security controls should be applied to Restricted data.

B. Private Data

Data should be classified as **Private** when the unauthorized disclosure, alteration or destruction of that data could result in a moderate level of risk to the University or its affiliates. By default, all Institutional Data that is not explicitly classified as Restricted or Public data should be treated as Private data. A reasonable level of security controls should be applied to Private data.

C. Public Data

Data should be classified as **Public** when the unauthorized disclosure, alteration or destruction of that data would result in little or no risk to the University and its affiliates. Examples of Public data include press releases, course information and research publications. While little or no controls are required to protect the confidentiality of Public data, some level of control is required to prevent unauthorized modification or destruction of Public data.

Classification of data should be performed by an appropriate Data Steward. Data Stewards are employees of the University who oversee the lifecycle of one or more sets of Institutional Data. See the Information Security Plan's *Roles and Responsibilities* for more information on the Data Steward's role and associated responsibilities.

9.3 Data Collections

Data Stewards may wish to assign a single classification to a collection of data that is common in purpose or function. When classifying a collection of data, the most restrictive classification of any of the individual data elements should be used. For example, if a data collection consists of a student's name, address and social security number, the data collection should be classified as Restricted even though the student's name and address may be considered Public information.

9.4 Reclassification

On a periodic basis, it is important to reevaluate the classification of Institutional Data to ensure the assigned classification is still appropriate based on changes to legal and contractual obligations as well as changes in the use of the data or its value to the University. This evaluation should be conducted by the appropriate Data Steward. Conducting an evaluation on an annual basis is encouraged; however, the Data Steward should determine what frequency is most appropriate based on available resources. If a Data Steward determines that the classification of a certain data set has changed, an analysis of security controls should be performed to determine whether existing controls are consistent with the new classification. If gaps are found in existing security controls, they should be corrected in a timely manner, commensurate with the level of risk presented by the gaps.

9.5 Calculating Classification

The goal of Information Security, as stated in the University's Information Security Plan, is to protect the confidentiality, integrity and availability of Institutional Data. Data classification reflects the level of impact to the University if confidentiality, integrity or availability is compromised.

Unfortunately, there is no perfect quantitative system for calculating the classification of a particular data element. In some situations, the appropriate classification may be more obvious, such as when federal laws require the University to protect certain types of data (e.g., personally identifiable information). If the appropriate classification is not inherently obvious, each security objective will be considered using the following table as a guide. The table is an excerpt from Federal Information Processing Standards (FIPS) Publication 199, published by the National Institute of Standards and Technology (NIST), which discusses the categorization of information and information systems.

	Potential Impact		
Security Objective	**Low**	**Moderate**	**High**
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information.	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

As the total potential impact to the University increases from Low to High, the classification of data should become more restrictive moving from Public to Restricted. If an appropriate classification is still unclear after considering these points, the Information Security Office should be immediately contacted for assistance.

10. Appendix B – Definitions

- ***Agent,*** for the purpose of this plan, is defined as any third-party who has been contracted by Howard University to provide a set of services and who stores, processes or transmits Institutional Data as part of those services.

- ***Electronic Media*** is defined as media that records and/or stores data using an electronic process. This includes but is not limited to internal and external hard drives, CDs, DVDs, USB drives, magnetic tapes and SD cards.

- ***Information System*** is defined as any electronic system that can be used to store, process or transmit data. This includes but is not limited to servers, desktop computers, laptops, multi-function printers, PDAs, smartphones and tablet devices.

- ***Institutional Data*** is defined as any data that is owned or licensed by Howard University.

- ***Least Privilege*** is an Information Security principle whereby a user or service is provisioned the minimum amount of access necessary to perform a defined set of tasks.

- ***Media*** is defined as any materials that can be used to record and/or store data. This includes but is not limited to electronic media (see definition above), paper-based media and other written media (e.g., whiteboards).

- ***Multi-factor Authentication*** is the process by which more than one factor of authentication is used to verify the identity of a user requesting access to resources. There are three common factors of authentication: something you know (e.g., password, pin, etc.), something you have (e.g., smartcard, digital certificate, etc.) and something you are (e.g., fingerprint, retinal pattern, etc.). Use of username and password combination is considered single-factor authentication, even if multiple passwords are required. Username and password used in conjunction with a smartcard is two-factor authentication. Multi-factor authentication represents the use of two or three factors.

- ***Privileged Access*** is defined as a level of access above that of a normal user. This definition is intentionally vague to allow the flexibility to accommodate varying systems and authentication mechanisms. In a traditional Microsoft Windows environment, members of the Local Administrators, Domain Administrators and Enterprise Administrators groups would all be considered to

have privileged access. In a traditional UNIX or Linux environment, users with root level access or the ability to undo would be considered to have privileged access. In an application environment, users with ‘super-user’ or system administrator roles and responsibilities would be considered to have privileged access.

HOWARD FORWARD