

HOWARD UNIVERSITY

Series: Information and Technology
Title: CYBERSECURITY PROGRAM
Responsible Officer: Executive Vice President and Chief Operating Officer
Delegated to the Chief Information Officer
Responsible Office(s): Office of the Chief Operating Officer
Office of Audit and Compliance
Office of Procurement and Contracting
Effective Date: Program Approved on September 9, 2024

I. POLICY STATEMENT

This policy is designed to establish a cybersecurity program to protect Howard University (HU) information and information systems from unauthorized access, loss or damage while supporting the open, information-sharing needs of our academic culture. University information may be verbal, digital and/or hardcopy, individually controlled or shared, stand-alone or networked, and used for administration, research, teaching, or other purposes. Standards and procedures related to the implementation of this Cybersecurity policy will be developed and published separately.

This policy will be reviewed annually and updated as necessary by the Responsible Officer.

II. RATIONALE

Cybersecurity is necessary to protect electronic information from threats to ensure continuity, minimize risks, and maximize university opportunities. Cybersecurity is not the purview of any one functional group. The cooperation of all departments, schools, and colleges is required to secure Howard's environment, the information used to achieve specific goals, and satisfy compliance requirements.

The Enterprise Technology Services Cybersecurity (ETS Cyber) division manages the cybersecurity program at HU by engaging directly with the departments, schools, and colleges to support the mission of academic, clinical, research, and administrative excellence by ensuring HU information system assets and data are protected at a level commensurate with their classification, sensitivity, and criticality.

III. ENTITIES AFFECTED BY THIS POLICY

This policy applies to:

1. HU information systems (IS), contracted information technology (IT) services, or any IS that creates, collects, uses, processes, stores, maintains, disseminates, discloses, transmits

or disposes of HU information, controlled unclassified information (CUI), personally identifiable information (PII), or electronic protected health information (ePHI);

2. Any information system funded directly or indirectly through a grant or contract for HU, any information system/service connected to an HU-managed information system or service (e.g., cloud application using HU Azure Active Directory for authentication); and
3. Howard employees, faculty and students, contingent/contract personnel, and other authorized users of HU assets, hereafter referred to as “HU Users”.

DEFINITIONS

- A. Asset (HU Asset) - Anything of value, virtual or physical, to HU that helps achieve the mission and objectives. This includes but is not limited to cloud environments or services, applications, hardware, software or the enterprise network.
- B. Information System (IS) - A combination of software, hardware, and telecommunication networks used to collect, process, maintain, use, share, disseminate, or dispose of information.
- C. Incident - A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices that actually or imminently jeopardizes the confidentiality, integrity or availability of an information system/service. An incident may be intentional or unintentional.
- D. Endpoint – Any desktop computer, laptop, smartphone, tablet, or Internet of Things (IoT) device that connects to the HU network or is used to access an HU Asset.
- E. Endpoint Security – The process of protecting endpoints from malicious threats and cyberattacks. This protection is implemented using software like antivirus or monitoring tools along with specific configurations that enforce secure management and usage of assets.
- F. Least Privilege – The process of providing access to the minimum amount of information necessary to meet operational or job requirements.
- G. Software as a Service (SaaS) – An application that is hosted and managed in the cloud by a service provider. HU is considered a customer of the service and has minimal control over the configuration of the supporting operating system or functionality of the application. The service provider is responsible for basic security of the application and the protection of any Howard information it handles.

IV. POLICY PROCEDURES

The Howard Cybersecurity Program will:

- Provide appropriate security for PII, ePHI, financial information, research activities and any information created, collected, processed, stored, transmitted, disseminated, or disposed of by or on behalf of HU;
- Maintain policies that address the wide array of technical functions and compliance requirements to support the effective operation of the Cybersecurity Program;

- Implement best security practices based on a risk-based analysis and cost/benefit approach;
- Provide training and awareness for any individual with authorized access to HU information systems or services; and
- Define the appropriate activities in response to a security incident or a disruption of IT services due to a security incident.

A. GOVERNING FRAMEWORKS & AUTHORITIES

The HU Cybersecurity Program will follow National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, Cybersecurity and Privacy Frameworks* in combination with the NIST Cybersecurity Framework (CSF) and the Control Objectives for Information and Related Technology (COBIT) 2019, as promulgated by ISACA (Information Systems Audit and Control Association) as appropriate to support HU.

This policy aligns with the baseline IT requirements outlined in the Gramm-Leach-Bliley Act (GLBA), Health Insurance Portability and Accountability Act (HIPAA) Security Rule, Family Educational Rights and Privacy Act (FERPA), and Criminal Justice Information Services (CJIS).

B. ROLES & RESPONSIBILITIES




1. The Chief Operating Officer (COO) is responsible for providing adequate resources and fostering a commitment to a Cybersecurity Program that meets the vast needs of HU.
2. The Associate Vice President and Chief Information Officer (CIO) is responsible for enforcing and assuring an effective Cybersecurity Program exists to support HU.
3. The Chief Information Security Officer (CISO) is responsible for the overall management and technical compliance of the Cybersecurity Program.
4. The Chief Audit and Compliance Officer is responsible for conducting internal control audits that measures the Cybersecurity Program against published policies, procedures, and guidelines. The frequency and nature of these reviews are based on the risk and criticality of the resource, major changes, or new State or Federal regulations.
5. The Privacy Officer is responsible for identifying when information requires higher levels of protection based on the Privacy Act and HIPAA requirements.
6. The CUI-Senior Administrative Official is responsible for identifying when information requires higher levels of protection based on the presence of controlled unclassified information (CUI) and the applicability of information security requirements required for the protection of CUI.
7. The Associate Vice President and Chief Procurement Officer has the responsibility of holding vendors responsible for complying with their legal and contractual obligations, including meeting cybersecurity, privacy, confidentiality and classified document

requirements applicable to HU vendors, including for contracted services that have any IT component.

8. Cabinet leadership is responsible for their divisions' compliance with this and other related policies, guidelines, or procedures.
9. Departments, schools and colleges are responsible for identifying information in their possession which must be classified as Restricted or Private, in accordance with the procedures in this Policy.
10. HU Users will adhere to this and other related policies especially when accessing PII, ePHI, financial information, Restricted or Private information and supporting systems.

C. INFORMATION CLASSIFICATION LEVELS

Information classification, in the context of cybersecurity, is the classification of data based on its level of sensitivity and the impact on HU should that data be disclosed, altered, or destroyed without authorization. Information classification 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:

Classification	Definition
	Data is classified as Restricted when the unauthorized disclosure, alteration, or destruction of that data could cause a significant risk to the University or its affiliates, including via regulatory or contractual obligations. Restricted data includes data protected by state or federal privacy regulations and data protected by confidentiality or contractual agreements. The highest level of security controls is applied to Restricted data.
	Data is 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, including via regulatory or contractual obligations. By default, all Howard data that is not explicitly classified as Restricted or Public is considered Private. A reasonable level of security controls is applied to Private data.
	Data is 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 Directory Information (as defined by the Student Privacy Rights Policy), 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.

HU Users are responsible for complying with any security controls imposed on the information, at any classification level, to which they have access.

1. Types of Restricted Information

At a minimum, the following Howard information is classified as Restricted. This list does not encompass all types of data which may be classified as Restricted.

Type of Information	Definition	Examples
Authentication Verifier	An Authentication Verifier is a piece of information that is held in confidence by an individual and used to prove that the person is who they say they are. An Authentication Verifier may also be used to prove the identity of a system or service.	Passwords, pass codes, shared secrets, cryptographic private keys, multifactor authentication apps
Controlled Unclassified Information (CUI)	Government created or owned unclassified information that requires safeguarding or dissemination controls consistent with applicable laws, regulation and government wide policies that is not deemed classified as defined by Executive Order 13526, <i>Classified National Security Information</i> .	Restricted data sets or technical data from government agencies, information created by Howard for the government as part of a contract Federal student aid information, specifically the Institutional Student Information Record (ISIR)
Covered Financial Information	Nonpublic personal information about a student or other third party who has a continuing relationship with Howard, where such information is obtained in connection with the provision of a financial service or product by Howard, and that is maintained by or on behalf of Howard as required by the Gramm-Leach-Bliley Act (GLBA).	Student name, address, and parent's financial information, Student loans, disbursement of financial aid, payment plans, tax return information
Electronic Protected Health Information (ePHI)	<p>ePHI is defined as any individually identifiable health information that is transmitted by electronic media and/or maintained in an information system.</p> <p>Electronic media means:</p> <p>(1) Electronic storage media including memory devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card; or</p> <p>(2) Transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the internet (wide-open), extranet (using internet technology to link a business with information accessible only to collaborating parties), leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be transmissions via electronic media, because the information being exchanged did not exist in electronic form before the transmission</p>	Electronic health records, patient telemedicine consultations, health insurance information, health information that is collected and/or stored in a SaaS, on a hard drive or external USB storage.

Type of Information	Definition	Examples
Export Controlled Materials	Export Controlled Materials is defined as any information or materials that are subject to United States export control regulations including, but not limited to, the Export Administration Regulations (EAR) published by the U.S. Department of Commerce and the International Traffic in Arms Regulations (ITAR) published by the U.S. Department of State. See the Office of Regulatory Research Compliance on Export Control for more information.	Information/research that may fall into any of the following categories: (0) Nuclear Materials, Facilities and Equipment, and Miscellaneous; (1) Materials, Chemicals, "Microorganisms," and Toxins; (2) Materials Processing; (3) Electronics Design, Development and Production; (4) Computers; (5) Telecommunications; (6) Sensors; (7) Navigation and Avionics; (8) Marine; (9) Propulsion Systems, Space Vehicles, and Related Equipment
Personal Data from European Union (EU)	Any personal data that is collected from individuals in the European Economic Area (EEA) countries is subject to the EU's General Data Protection Regulation (GDPR) which defines personal data as any information that can identify a natural person, directly or indirectly, by reference to an identifier such as: <ul style="list-style-type: none"> • Name • An identification number • Location data • An online identifier • One or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person 	Any HU student or employee records who identify as citizens of the EU
Personally Identifiable Information (PII)	PII is information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.	Full Name in combination with social security number, driver's license, or medical records.

2. Sharing and Reporting Restricted Information

Sharing of Restricted information within the University is permissible if required to meet HU's legitimate business needs. Except as otherwise required by law (or for purposes of sharing between law enforcement entities), no Restricted information may be disclosed to parties outside the University, including contractors, without the proposed recipient's prior written agreement (i) to take appropriate measures to safeguard the confidentiality of the Restricted information; (ii)

not to disclose the Restricted information to any other party for any purpose absent the University's prior written consent or a valid court order or subpoena; and (iii) to notify the University in advance of any disclosure pursuant to a court order or subpoena unless the order or subpoena explicitly prohibits such notification. In addition, the proposed recipient must abide by the requirements of this policy.

Prior to processing, storing, receiving, or transmitting Restricted information, a Software as a Service (SaaS) solution must undergo evaluation by ETS Cyber and/or the Office of Audit and Compliance. Reviews will be conducted as needed to verify ongoing compliance with safeguarding Restricted information.

Federal and State laws require that unauthorized access to certain Restricted information must be reported to appropriate agencies. The Chief Information Security Officer (CISO) has the responsibility of working with the Office of the General Counsel (OGC), as defined in the Incident Response Plan, to report the incident to the appropriate external parties.

3. Private, Public or Undefined Information

Most information handled within the Howard network enterprise is either Private or Public. Information classified as Private is restricted from leaving the Howard enterprise, meaning it will not be shared with non-HU Users. ETS Cyber will define the technical security controls to ensure information classified as Private is prevented from leaving an ETS managed information system. It is the responsibility of the department or school to define when and what information should have a Private classification.

Departments, schools and colleges should coordinate with ETS Cyber before the initial purchase or renewal of any SaaS that will handle Private information. Ongoing compliance verification will occur during contract renewal or as needed.

Public information will inherit basic security protections from the IS without any additional security controls. Departments, schools and colleges are encouraged to define how they will handle information classified as Public. By default, information not explicitly defined as Restricted or Private is Public.

If a department, school or HU User is unsure about how to classify information they should contact ETS Cybersecurity for assistance.

4. Transit, Storage and Backups

To ensure the security of HU information classified as restricted or private, it must be fully encrypted when at rest. Restricted and Private information can only be stored in an ETS-managed IS/service or a fully vetted SaaS. ETS-managed IS and storage are fully encrypted and continuously backed up.

If Howard information is stored outside of an ETS-managed IS or a fully vetted SaaS, the department, school, or HU User assumes the responsibility for ensuring that the information remains fully encrypted at rest and is backed up as needed to meet operational requirements.

D. GENERAL SECURITY REQUIREMENTS

The following security requirements apply to any HU Asset or contracted IT services managed directly or indirectly by ETS, a department or school. The objective of these protections is to protect the HU brand, the people and the information they use. Details related to these requirements are defined in other policies or procedures.

1. *Access Control:* Authorized HU Users will use an individual account with multifactor authentication (MFA) enabled whenever possible to access HU Assets, information or IT services.
2. *Audit and Accountability:* Information systems and services are required to maintain audit logs that capture authorized/unauthorized access to the system and the information.
3. *Configuration Management/Maintenance:* Regular updates and patches for systems and software will be issued to protect against known vulnerabilities to maintain a secure baseline. An HU Asset or IT service will not be more than one version (N-1) behind the most up-to-date version. HU Users are required to implement updates when requested by the IS.
4. *Cybersecurity Training and Awareness:* ETS Cyber will provide reoccurring cybersecurity training to all HU Users. HU Users are required to participate in and complete any training requested by ETS Cyber.
5. *Data Destruction:* Establish procedures for the secure disposal or destruction of information that aligns with 400-003 Record Retention and Destruction Policy.
6. *Data Encryption:* Any HU data will be encrypted in transit, at rest and whenever possible while in use to protect against unauthorized access.
7. *Endpoint Protection:* Endpoints that are accessing or processing HU information will have security protections (e.g., firewalls, antivirus, monitoring agent, etc.) commensurate with the type of information being processed.
8. *Incident Response Plan:* A comprehensive incident response plan has been developed by ETS that promptly addresses and mitigates the effects of security incidents across the enterprise. Each department and school must develop a tailored incident response plan, detailing their specific procedures for responding to incidents that disrupt their standard operations. HU Users are required to comply with these plans and any directives they receive from ETS or a department or school in accordance with these plans.
9. *Physical Security:* Prevent unauthorized physical access to information systems, storage and restricted areas. HU Users are prohibited from accessing information systems, storage, and restricted areas which they are not explicitly authorized to access.
10. *Risk Assessment:* IT systems and services will complete an annual risk assessment with the goal of identifying potential cybersecurity threats and vulnerabilities.

11. *Security Assessment*: Perform periodic security assessments, penetration testing, and vulnerability scans to evaluate the effectiveness of security measures.
12. *Vendor Management*: ETS and Procurement will ensure that third-party service providers adhere to Howard defined security standards and are contractually obligated to protect HU information.

1. Exemption

Departments, schools and colleges may submit an exemption request to ETS Cybersecurity for any of the security requirements listed above. Each exemption request must provide the following information:

- IS or service for which the exemption is sought
- Purpose of IS or service or how it is used
- Number of users for the IS or service, and the users that require the exemption
- Business Justification for the exemption
- Any proposed mitigation measures to ensure the exemption will not unnecessarily increase the vulnerability of HU

The request for the exemption will be reviewed by the CISO and submitted to the CIO and Chief Audit and Compliance Officer for approval. Submission of an exemption is not an automatic approval. The CISO, CIO, and Chief Audit and Compliance Officer reserve the right not to grant a requested exemption, limit the duration or applicability of the requested exemption, or otherwise take any measures necessary to mitigate the impact of the requested exemption. The CISO, CIO, and Chief Audit and Compliance Officer are not required to provide a justification for taking any of these actions, although they may provide an explanation for the refusal or mitigation measures imposed.

E. PERFORMANCE MANAGEMENT

The Howard Cybersecurity Program will use the COBIT 2019 process capability scheme to measure the effectiveness and maturity of the program. The program maturity is based on six high level functional areas: Govern, Identify, Protect, Detect, Respond and Recover. At the end of each fiscal year the CISO will provide a report to the CIO and COO on the current maturity of the cybersecurity program.

Function	Description
Govern	Establish and monitor the cybersecurity risk management strategy, expectations and policy.
Identify	Help determine the current cybersecurity risk to Howard.
Protect	Use appropriate safeguards to prevent or reduce cybersecurity risk.

Detect	Find and analyze cybersecurity attacks and compromises.
Respond	Act regarding a detected cybersecurity incident
Recover	Restore assets and operations that were impacted by a cybersecurity incident

The following table defines the different process capability levels and how they can be used.

Level	Name	Capability	
0	Incomplete	The process is not implemented or fails to achieve its purpose.	Instance View – Outcomes from these levels are limited to the specific process.
1	Performed	The implemented process achieves its purpose.	
2	Managed	The level 1 performed process is now implemented in a managed fashion (planned, monitored, and adjusted) and the outcome is established, controlled and maintained.	
3	Established	The level 2 managed process is now implemented using a defined process that can achieve its process outcomes.	Enterprise View – Outcomes from these levels are used for decision making and governance.
4	Predictable	The level 3 established process now operates within defined limits to achieve its process outcomes.	
5	Optimizing	The level 4 predictable process is continuously improved to meet relevant current and projected business goals.	

F. RELATED POLICES, PROCEDURES, AND GUIDELINES

There are several policies and procedures that further define the key aspects of this policy. It is the responsibility of each HU User to stay up to date on all applicable policies. The most current policies will be listed at <https://technology.howard.edu/> and <https://secretary.howard.edu/policy-office> .

- Acceptable Use of University Information Resources, Data and Communication Services
- Computer Security Incident Response
- Cybersecurity Awareness Training (CSAT)
- Howard University Email Management
- Information Technology (IT) Governance

- Research Security Policy – Controlled Unclassified Information (CUI)

V. INTERIM POLICIES

There are no interim policies.

VI. SANCTIONS

Failure to follow this policy or any other approved University policy may result in disciplinary action.

VII. WEBSITE RESOURCES

[Policy Office | Howard University Office of the Secretary](#)

[Family Educational Rights and Privacy Act \(FERPA\)](#)

[GLBA Safeguard Rule](#)

[CJIS Security Policy 2022 v5.9.1 — FBI](#)

[Summary of the HIPAA Security Rule | HHS.gov](#)

[NIST 800-171: Protecting Controlled Unclassified Information in Nonfederal Systems \(nist.gov\)](#)

[The NIST Cybersecurity Framework \(CSF\) 2.0](#)