HOWARD UNIVERSITY POLICY

Policy Number:	700-103, Information Technology
Policy Title:	Computer Security Incident Response Policy
Responsible Officer:	Chief Information Officer
Responsible Office:	Office of the Chief Operating Officer
Effective Date:	April 10, 2023

I. POLICY STATEMENT

The purpose of this policy is to establish the rules that govern the response to Computer Security Incidents, hereafter referred to as "security incidents", that occur at Howard University. The Enterprise Technology Services (ETS) has the overall responsibility for responding to security incidents that are either reported by HU Users or discovered as part of the continuous monitoring of the HU network.

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

II. RATIONALE

As a higher education institution Howard University is a target for cyber threat actors. When a security incident happens HU must be ready to quickly response and recovery. This policy will define the criteria for those activities.

This Policy applies to Computer Security Incidents that pose a threat to University Information Systems or University Data. This Policy does not include the following:

- Losses of or damage to a University Information System or University Data caused by natural disasters or power failures;
- Detected vulnerabilities to University Information Systems; or,
- Personally-owned computer assets that do not contain University Data

III. ENTITIES AFFECTED BY THIS POLICY

Any authorized user of Howard information systems (IS) or services and ETS managed assets.

IV. DEFINITIONS

A. Asset (HU Asset) - anything of value to HU that helps achieve the HU mission and objectives, specifically cloud environments or services, applications, hardware,

software or the enterprise network.

B. HU User – an authorized user of any Howard IS this includes students, faculty, employees, and contingent workers.
C. Information System (IS) - a combination of software, hardware, and telecommunication networks used to collect, process, maintain, use, share, disseminate, or dispose of information.
D. Mission Critical - an IS that houses information to which the loss, misuse, disclosure, or unauthorized access to or modification of, would have a debilitating impact on the mission of Howard.
E. Unauthorized Access - A person who gains logical or physical access without permission to a HU Asset.

V. POLICY PROCEDURES

Security incident is any activity that (1) actually or imminently jeopardizes (without lawful authority) the integrity, confidentiality, or availability of information or an IS; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies. If a security incident impacts one HU User, one department or school or the entire HU enterprise the response procedures are the same.

A. SECURITY INCIDENT CLASSIFICATION

The University will classify the following occurrences as security incidents:

- A suspected, attempted, successful, or imminent threat to the confidentiality, integrity, and/or availability of HU information/data;
- Interference or unauthorized access to a HU IS; or
- A violation, or imminent threat of violation, of HU asset, acceptable use, IT related policies, standards, and/or procedures.

A security incident will be classified as either Major, Moderate, or Minor based on the following factors:

- Functional impact the security incident has on affected HU IS and future functional impact if it is not immediately contained;
- Effect of security incident on the confidentiality, integrity, and availability of HU information and how this information exfiltration will impact the University's overall mission or reputation; and,
- The effort necessary to recover from the security incident weighed against the value the recovery effort will create and any requirements related to the response activities.

Major Security Incidents pose a substantial threat to University Information Systems or University Data and meet the following criteria:

- Involves potential, accidental, or otherwise unauthorized access or disclosure of Restricted or Private information;
- Involves legal issues including criminal activity or may result in litigation;
- Has or may cause severe disruption to mission critical services; or,
- Is likely to cause harm to the University's reputation.

Security Incidents not classified as Major will be classified as Moderate or Minor based on the number and criticality of HU IS, records, persons, or accounts affected.

B. SECURITY INCIDENT RESPONSE

Security incident response at Howard will follow established industry standards such as the National Institute of Standards and Technology (NIST) Special Publication 800-61, *Computer Security Incident Handling Guide* or current equivalent.

The University will measure the success of its Security Incident Response capabilities by developing appropriate metrics and testing Security Incident Response capabilities at least annually.

Major Security Incidents will require investigation by a Incident Response Team (IRT). The purpose of the IRT manage the response activities. The IRT will at a minimum, include a Team Manager and an Incident Lead, who are identified by the Chief Information Officer (CIO). Depending on the impact of the security incident additional representation may be added at the direction of the Chief Operating Officer or executive leadership.

- The Team Manager is responsible for acting as a liaison with executive leadership and other teams and organizations, defusing crisis situations, and ensuring that the team has the necessary personnel, resources, and skills.
- The Incident Lead is responsible to serve as the primary point-of-contact for Incident Response and for oversight of the quality of the team's technical work.
- Additional roles, including representation from legal, communications, human resources and functional business units or schools impacted, may also be added.

The IRT will respond to Major Security Incidents according to an approved computer security incident response plan, which includes conducting the following activities:

- Determining the extent, cause, and damage of the security incident;
- Directing the recovery, containment, and remediation of security incident, which may include authorizing and expediting changes to HU ISs or services;
- Monitoring HU ISs and retrieving communications or other relevant records related to specific users, including login session data and the content of individual communications;
- Notifying the appropriate individuals/groups to participate and identifying their roles. This includes coordinating communications with external parties when existing

agreements place responsibility for Security Incident investigations on the external party;
- Providing status updates to specific individuals, groups, and/or the entire University.
    - In coordination with Howard University Communications, the IRT may have a need to prepare several communication methods and select the methods that are appropriate for a Major Security Incident;
- Coordinating and sharing information with law enforcement if necessary; and,
- Coordinating and sharing information with any HU external partners as part of any formal agreement of security incident notification.

C. SECURITY INCIDENT REPORTING

Anyone who has knowledge or suspects that a Security Incident has occurred, must report the security incident immediately to the ETS Help Desk by calling 202-806-2020 or email ets-cybersecurity@howard.edu and huhelpdesk@howard.edu.

Failure to report an actual or suspected security incident is a violation of this Policy.

If the security incident is reasonably expected to cause significant harm to University employees or students, the University will make best efforts to notify those individuals whose Personally Identifiable Information (PII) or Electronic Protected Health Information (ePHI) may have been put at risk. Factors to consider in making this determination include:

- Legal duty to notify;
- Length of compromise;
- Human involvement;
- Sensitivity of compromised data; and,
- Existence of evidence that data was compromised.

VI. INTERIM POLICIES

There are no interim policies.

VII. SANCTIONS

Failure to follow this policy or any other approved University policy may result in disciplinary action, including termination of employment.

VIII. WEBSITE ADDRESS

- Policy Office | Howard University Office of the Secretary
- 700-105, Cybersecurity Policy
- 400-003, Record Retention and Destruction Policy