HOWARD UNIVERSITY POLICY

Policy Number:	700-102, Information Technology
Policy Title:	Cybersecurity Awareness Training Policy (CSAT)
Responsible Officer:	Chief Information Officer
Responsible Office:	Office of the Chief Operating Officer
Effective Date:	August 2, 2023 April 10, 2023 (Original)

I. POLICY STATEMENT

Enterprise Technology Services Cybersecurity (ETS Cyber) division strives to keep the Howard community cyber aware of the latest cyber security threats, safe computing practices, and relevant information. Higher education is one of most targeted industry for cyber attacks which requires members of this industry to be cyber aware this is accomplished through continuous cybersecurity training.

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

II. RATIONALE

Howard University handles an array of information ranging from public to financial to protected health information. This massive inventory of information requires cybersecurity awareness training (CSAT). This policy will outline the frequency of CSAT and the circumstances when additional training is required.

III. ENTITIES AFFECTED BY THIS POLICY

Any authorized user of Howard information systems (IS) or services is required to complete CSAT as defined in this policy.

IV. DEFINITIONS

A. Credible Threat Intelligence – threat information from a reliable source that has been aggregated, transformed, analyzed, interpreted, or enriched to provide the necessary context for making IT and cyber related decisions.

B. 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.

C. HU User – an authorized user of any Howard IS this includes students, faculty, employees, and contingent workers.

D. Information System (IS) - a combination of software, hardware, and telecommunication networks used to collect, process, maintain, use, share, disseminate, or dispose of information.

E. Learning Management System (LMS) – a software application for the

administration, documentation, tracking, reporting, automation, and delivery of educational courses, training programs, materials or learning and development programs.

F. Phishing - the fraudulent practice of sending emails or other messages purporting to be from reputable companies or individuals in order to trick HU Users into revealing information, such as passwords and credit card numbers, to either gain access to an IS or steal an identity.

V. POLICY PROCEDURES

The HU User and the information they access will determine the type of training they receive. CSAT training will occur on the enterprise identified Howard LMS.

A. INITIAL / RECURRING TRAINING

Any person hired to work at Howard as a full or part-time employee, student employee, contingent worker or faculty is required to complete initial CSAT before having access to any HU Asset. Recurring training will occur using the table below, unless the Chief Information Security Officer (CISO) deems additional training is necessary based on HU User behavior.

HU Users or Role	Recurring Training Schedule
All (except students)	Quarterly
Students	At the start of each semester
Privileged Users	Quarterly
Executive Leadership	Semi-annual
Research Principal Investigators	Annually

B. PHISHING EXERCISES AND TRAINING

Phishing is the most used tactic to gain access to an HU IS. Even though there are technical controls in place to reduce the number of phishing attempts, the best defense is an educated HU User. Specific phishing training is part of the CSAT; ETS Cyber will run phishing exercises to test the effectiveness of the training. All HU Users will participate in quarterly phishing exercises.

The following table defines the departments or schools that require more frequent targeted phishing training.

HU User	Phishing Exercise Training Schedule
Health Science Students & Faculty	Quarterly
Office of Human Resources	Monthly
Office of the Chief Financial Officer	Monthly
All	As needed if the exercise click rate is higher than the established target for the quarter or if there's an uptick in HU Users clicking on phishing email attempts.

C. TRAINING PLAN

The CISO in coordination with the Chief Audit and Compliance Officer will identify the subject areas that CSAT should focus on at the start of the academic fiscal year. Internal and External audits along with cybersecurity trends will drive the focus areas for training. At a minimum CSAT will cover phishing, identity protection, malware/ransomware, and privacy protection.

1. Reporting

The CISO is responsible for providing monthly, quarterly, and yearly training completion, incomplete training and phishing exercise results to the Chief Information Officer (CIO) and Chief Audit & Compliance Officer.

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.

1. Non-Compliance Actions for Mandatory Training

All HU Users are expected to complete mandatory training by the identified due date. Incomplete training is part of the monthly, quarterly, and yearly reporting. The following actions will occur each time the due date is missed for mandatory training.

> **1st Missed Due Date:** The first time mandatory training is not completed by the due the HU user and their supervisor or department chair are notified by the CISO via email.
>
> **2nd Missed Due Date:** The second time mandatory training is not completed by the due the HU user, their supervisor or department chair and Human Resources are notified by the CISO, CIO or Chief Audit & Compliance Officer via email.
>
> **3rd Missed Due Date:** The third time mandatory training has not been completed by the due date the individual's access to HU assets will be disabled 72 hours after being notified. The CISO, CIO or Chief Audit & Compliance Officer will send notification via email to the HU User, their supervisor or department chair, Human Resources and the Executive Cabinet member to whom they report.

VIII. WEBSITE ADDRESS

Policy Office | Howard University Office of the Secretary

Howard University Employee Handbook

Howard University Faculty Handbook