# HOWARD UNIVERSITY POLICY

| | |
|---|---|
| **Policy Number:** | 700-002 Information and Technology |
| **Policy Title:** | ACCEPTABLE USE OF UNIVERSITY INFORMATION RESOURCES, DATA, AND COMMUNICATION SERVICES |
| **Responsible Officers:** | Chief Operating Officer delegated to the Chief Information Officer |
| **Responsible Office:** | Office of the Chief Information Officer |
| **Effective Date:** | June 29, 2011; August 2023 (Revised Interim) |

## I. POLICY STATEMENT

The Howard University (hereinafter, "HU" or "the University") provides computing and network related technology and information resources ("Computing Systems and Services") to its community to support the university's academic and research mission as well as its business operations.

This policy establishes the acceptable use, roles and responsibilities of HU Computing Systems and Services to ensure that such resources are used for their intended purpose while respecting the rights of other computer users, the integrity of the technological infrastructure, and relevant license and contractual agreements.

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

## II. RATIONALE

The purpose of this policy is to define acceptable use of the University's technology and information resources. These rules are in place to protect the University and those authorized to use its systems. Inappropriate use exposes the University to risks including but not limited to virus attacks, compromise of network systems and services, legal issues and tarnished reputation.

This policy applies to all Computing Systems and Services owned or operated by or on behalf of the University. Anyone authorized access in any capacity is responsible for adhering to this policy.

It is the responsibility of every user to know these guidelines, and to conduct their activities accordingly.

## III. ENTITIES AFFECTED BY THIS POLICY

This policy applies to all individuals who access, use, or control University electronic information resources. Those individuals include, but are not limited to University and Hospital staff, faculty, students, residents, volunteers, alumni, temporary staff, contractors

and consultants working on behalf of the University, guests, visitors, and individuals affiliated with other institutions and organizations ("Authorized Users").

This policy will be implemented by Enterprise Technology Services (ETS) and digitally delivered to each account user upon first attempt to access the University network with new user account credentials, and/or during staff orientation.

## IV. DEFINITIONS

- **Authorized Users** – All faculty, staff, students, contractors, consultants, temporary workers, and guests as well as those who represent themselves as being associated with the university and who make use of University computing systems and services.
- **Compromised** - Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred.
- **Computing Systems and Services** – Any equipment owned, operated or contracted by the university that is used in the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information electronically or via cloud-based systems, including printers, storage devices, computers, computer equipment, network equipment and systems and phone equipment and systems; and includes desktops, laptops, mobile phones, tablets, voice-over-internet protocol devices (VOIP), USB drives and other removable media, copiers, and the software that accesses, views, processes, transmits, stores or disposes of HU digital information.
- **FERPA** – Family Educational Rights and Privacy Act, as amended, sets forth requirements regarding the privacy of student records. Howard University is subject to FERPA's privacy requirements regarding the release of education records and access to these records.
- **HIPAA** – Health Insurance Portability and Accountability Act enacted to combat fraud and abuse in healthcare, as well as to improve healthcare systems by encouraging the electronic transfer of medical information. Howard University is subject to HIPAA's privacy requirements.
- **Personally Identifiable Information / Sensitive Information** – Privileged or proprietary information which, if compromised through unauthorized disclosure, alteration, corruption, loss, or misuse could cause serious harm to Howard University and its stakeholders. Sensitive Information can only be released to the subject of the information and to those within the University who have an official need-to-know, outside entities with the subject's written permission, and others as allowed by law. In many cases, the use of this information is protected by local, state and federal law, such as FERPA and HIPAA.
    - ***Protected Health Information (PHI)*** is considered sensitive as are ***Social Security numbers, Non-Directory student data***, and other personally identifiable information. See Appendix categories of Sensitive Information.
- **Personally Owned computers/devices** – Technology that is not owned or managed by Howard University.
- **Responsible Use** – Any action or behavior of an individual that does not cause accidental or unauthorized destruction, disclosure, misuse, or modification of or access to the information technology or computer resources owned or operated by the University.

## V. POLICY PROCEDURES

Authorized Users must adhere to HU's standards of academic and professional ethics, as included in HU's codes of conduct and employee handbooks and consider conduct in the use of Computing Systems and Services or any other computer system accessed by virtue of their affiliation with the University. Authorized Users agree to and are bound by this policy and all other applicable rules and regulations related to appropriate legal and ethical use of Computing Systems and Services.

The unauthorized use of Computing Systems and Services for personal or economic gain, political objectives, and any other activities that may jeopardize the University's reputation or regulatory compliance are prohibited.

### A. ACCEPTABLE USE

The University provides IT resources so that faculty, staff, students, and other members of the University community can pursue the missions of Howard University. In doing so, the University must protect the integrity, security, or functionality of IT resources. These protective efforts start by complying with all University policies, laws, regulations, contracts, and applicable laws.

1. **Institutional Use**

   The University computing resources are to be used primarily to advance the missions of education, research, clinical and public services, or for University related business. Authorized Users may use the computing resources only for purposes related to their studies, their responsibilities for providing instruction, the discharge of their duties as employees, their official business with the University, or other University sanctioned activity.

2. **Personal Use**

   Personal use of the University's information technology and digital resources, except for students enrolled at the University, should be incidental and kept to a minimum.

3. **Research Use**

   HU researchers obtain and share information and materials electronically that derive from a broad range of sources, including but not limited to organizations, federal agencies, websites, and specialized hardware and software. During a project, HU researchers may unintentionally be at risk of exposure to malware, or other vulnerabilities, which may degrade Computing Systems and Services and put HU research information at risk for fraud, theft, or misappropriation. Researchers who are actively using Computing Systems and Services to perform research of this nature are responsible for informing ETS before project initiation to ensure adequate security controls are in place.

### B. POLITICAL USE

As a 501(c)(3) organization, the University is prohibited from participating or intervening in any political campaign on behalf of or in opposition to a candidate for public office, and no substantial part of the University's activities may be directed to influencing legislation

(i.e., lobbying). Individuals may not use University technological resources, name, images, symbols or trademark for political purposes in a manner that suggests that the University itself is participating in a campaign, political activity or fundraising, endorses or opposes any candidate or political party. Any other use with respect to political activity must be permitted by applicable University policy and consistent with applicable laws.

Students and student organizations are permitted to independently engage in political or public interest activities.

## C. COPYRIGHT AND INTELLECTUAL PROPERTY

Authorized Users are prohibited from using Computing Systems and Services to violate the intellectual property rights of a third party. This includes copyright, trade secrets, patent or other intellectual property rights, as well as violation of similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products for which they are not appropriately licensed.

Additionally, Authorized Users are prohibited from using Computing Systems and Services to make or use unauthorized copies of copyrighted material including, but not limited to, music, movies, television shows, books, magazines, or software for which the university or the end user does not have an active license.

HU is required to adhere to the Digital Millennium Copyright Act and may report any instances of reported or identified copyright violations to the copyright holders and associated trade groups upon request.

## D. RESPONSIBILITIES OF THE UNIVERSITY

The University has the legal right, to access, preserve and review all information stored on or transmitted through its electronic services, equipment and systems. The University endeavors to afford reasonable privacy for individual users and does not access information created and/or stored by individual users on its IT Systems except when it determines that it has a legitimate operational need to do so. These reasons include but are not limited to:

1. Maintenance or improvement of computing resources or any other IT specific purpose.
2. Monitoring for viruses and other destructive computer programs.
3. Investigation of violation of University policy or by an authorized law enforcement or other federal, state, or local agency.
4. Where otherwise required by law.

### 1. PRIVACY

While ETS attempts to provide a reasonable level of privacy, users should be aware that the data they create, use or maintain on University systems remain the property of Howard University, and are subject to applicable University policies, and local, state, and federal regulations. Authorized Users are responsible for exercising good judgment regarding reasonable personal use. A reasonable level of privacy is balanced with the requirement to protect the University from risk.

## E. RESPONSIBILITIES OF USERS

In addition to the previous sections, Authorized Users of the University's Computing Systems and Services are expected to:

1. Report identified or suspected security issues/concerns to incidents to ETS Information Security Team (ets-infosec@howard.edu)
2. Use resources only for authorized purposes.
3. Prevent unauthorized access to their method of access to University Computing Systems and Services by not sharing usernames, passwords or multifactor authentication.
    - Understand that activities under an individual's own username and password are their own activities for which a user is accountable and responsible, unless determined the account was compromised.
4. Access only information to which they have been given authorized access or that is publicly available.
5. Use only legal versions of copyrighted software in compliance with vendor license requirements.
6. Be considerate while using shared resources. Refrain from monopolizing systems, overloading networks with excessive data, degrading services, or wasting computer time, connection time, disk space, printer paper, manuals, or other resources.

Authorized Users of the University's Computing Systems and Services WILL NOT:

1. Access pornography for purposes other than education or research.
2. Conduct illegal or unlawful activities, including but not limited to fraud, defamation, plagiarism, intimidation, forgery, impersonation, drug trafficking, sales and/or distribution, soliciting for illegal pyramid schemes, and computer tampering (e.g., spreading of computer viruses).
3. Violate HIPAA, FERPA and other applicable laws as they relate to computing resources and protecting personally identifiable information (PII).
4. Engage in any activity that is intended to harm (e.g., password cracking or hacking) systems or any information stored, creating or propagating malware (e.g., viruses, worms, or "Trojan horse" programs), attempting to circumvent security measures, disrupting services; damaging files; or making unauthorized modifications to University data.
5. Make or use illegal copies of copyrighted software, store such copies on University systems, or transmit them over University networks.
6. Use e-mail, social networking sites or tools, or messaging services in violation of laws or regulations or to harass or intimidate another person by way of libel, slander, defamation, or cyberbullying.
7. Waste shared computing or network resources, for example, by intentionally placing a program in an endless loop, printing excessive amounts of paper, or by sending chain letters or unsolicited mass mailings.
8. Use the University's systems or networks for commercial purposes; for example, by selling access to your User ID or by performing work for profit with University resources in a manner not authorized by the University, transmit commercial or personal advertisements, solicitations, endorsements, or promotions unrelated to the

business of the University.

9. State or imply that they speak on behalf of the University or use University trademarks and logos without authorization to do so.
10. Violate any applicable laws and regulations or University policies and procedures that govern the use of IT resources.
11. Maintain or store HU official/business information/data outside of the University's enterprise network without proper approval.

## VI. INTERIM POLICIES

There are no interim policies.

## VII. SANCTIONS

If an individual is found to be in violation of the Acceptable Use Policy, the University may take disciplinary action, including restriction of and possible loss of network privileges or more serious consequences, up to and including suspension, termination, or expulsion from the University. Individuals may also be subject to federal, state, and local laws governing many interactions that occur on the University's networks and on the Internet. These policies and laws are subject to change as state and federal laws evolve.

Student violations of the above policies will be handled through the Office of Student Rights and Responsibilities; other violations will be referred, as appropriate, to the University Human Resources or the University Police Department.

Violations of this policy by guests of the University and others with permission to use the University computing resources are to be reported to ETS and will be handled at the discretion of the administration. Sanctions may include, among other things, withdrawal of use privileges and reporting of the violation(s) to administrators of other computing resources and federal, state, or local law enforcement authorities.

## VIII. WEBSITE ADDRESS

University Policy Office

External Resources:

*Family Educational and Privacy Rights Act of 1974 (FERPA)*
*Health Insurance Portability and Accountability Act (HIPAA)*

**700-002 APPENDIX**
*SENSITIVE INFORMATION*

**Employee Information**

The following information is considered "sensitive" by Howard University:

- Social security number or other taxpayer ID
- Employee ID (Bison ID)
- Birth date
- Home phone number and address
- Personal contact information (e.g., email, phone number, etc.)
- Education and training
- Non-salary financial information (such as expense reimbursements, pension information, or fringe benefit value)
- Benefits information
- Health records
- Passwords or multifactor authentication
- Gender
- Ethnicity
- Citizenship / Citizen visa code
- Veteran and disability status
- Performance reviews or disciplinary actions
- Payroll time sheets
- Worker's compensation or disability claims

**Student Education Records**

The following information is considered "Non-Directory" information, as governed by FERPA, and cannot be released except under certain prescribed conditions.

- Social Security Number
- Student/Bison ID
- Grades
- Courses taken.
- Schedule
- Test scores
- Advising records
- Educational services received.

- Disciplinary actions
- Financial aid/grant information
- Student tuition bills
- Payment history

**Patient Health and Research**

The following information is governed by HIPAA and cannot be released except under certain prescribed conditions.

- Name
- Address information (street address, city, county, zip code)
- All elements of dates directly related to an individual except the year (e.g., date of birth, admission date, discharge date, date of death).
- All ages over 89 or dates indicating such an age, except that you may have an aggregate category of individuals 90 and older.
- Telephone number
- Fax number
- Email address
- Social security number
- Medical record number
- Health plan number
- Account number
- Certificate or license numbers
- Vehicle identification (e.g., VIN, serial numbers and license plate numbers)
- Device identification/serial numbers
- Universal resource locators (website URLs)
- Internet protocol addresses
- Biometric identifiers (e.g., fingerprints)
- Full face photographs and comparable images

**Any other unique identifying number, characteristic or code, Financial/ Credit Cards**

Any information obtained in payment of a good or service that would serve to identify an individual, including:

- Name
- Address
- Phone number
- Account balances
- ACH numbers.

- Bank account numbers
- Credit card numbers
- Credit rating
- Location of birth
- Driver's license information
- Income history
- Payment history
- Tax return information

Any information obtained during the processing of a credit card payment transaction that identifies individual consumers and their purchases, such as:

- Account number\credit card number
- Expiration date
- Name
- Address
- Social security number

**Other**

- Legal investigations conducted by the University.
- Sealed bids.
- Contract information between HU and third parties.
- Trade secrets or intellectual property, such as research activities.
- Location of HU assets.
- Identifying an individual to the specific subject about which the individual has requested HU library information or materials.
- Configuration of HU technology assets (e.g., network diagrams, firewall configurations, etc.)