HOWARD UNIVERSITY POLICY

Policy Number:	700-002
Policy Title:	ACCEPTABLE USE OF UNIVERSITY INFORMATION RESOURCES, DATA, AND COMMUNICATION SERVICES
Responsible Officer:	Office of the Chief Information Officer
Responsible Office:	Office of the Chief Information Officer
Effective Date:	June 29, 2011
Revision Date:	

I. POLICY STATEMENT

Howard University's ("the University's") network and computing technology provides information, data, and communication services. Responsible use of electronic information resources is necessary to create and maintain an open community of responsible users based on mutual respect and cooperation, commitment to the integrity of resources and data, and compliance with all University policies and federal, state, and local statutes.

The University's electronic information resources are provided to support the teaching, learning, clinical, and research missions of the University and their supporting administrative and healthcare functions. Inappropriate use of these electronic information resources threatens the atmosphere for the sharing of information, the free exchange of ideas, and a secure environment for access, use, edits and maintenance of electronic information resources.

This policy establishes the expectations for all users of the University's electronic information resources and data. It addresses the availability, integrity and confidentiality of resources in support of the University's missions, codifies appropriate usage, establishes the need for users to respect the rights of others and to be in compliance with other University policies, policies of external networks and resources, and all applicable federal, state, and local statutes.

II. RATIONALE

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, World Wide Web browsing, and FTP access, are University property. These systems are to be used for business purposes in serving the interests of the University.

The participation and support of every student, employee, (both faculty, staff) and affiliate (see Definition of User), who deals with information and/or information systems is necessary, to achieve effective security. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

The purpose of this policy is to delineate acceptable use of the University's technology and information resources. These rules are in place to protect the employee and the University. Inappropriate use exposes the University to risks including virus attacks, compromise of network systems and services, legal issues and reputation.

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.

IV. DEFINITIONS

A. **Computer -** An electronic device that performs logical, arithmetic, and memory functions by manipulating electronic or magnetic impulses, and that includes all input, output, processing, storage, software, and communication facilities that are connected or related to an electronic system or communication network.

   a. **Computer Hardware** - Any and all tangible or physical devices attached to or used in conjunction with a computer system.

   b. **Computer Network** - The interconnection of communication lines, including wireless connections, with a computer through remote terminals or a configuration consisting of two or more interconnected computers.

   c. **Computer Program** - An ordered set of instructions or statements that, when executed by a computer, causes the computer to process data.

   d. **Computer Resources** - Any and all computerized institutional data, computer hardware, and computer software owned by or operated at the University.

   e. **Computer Software** - A set of computer programs, procedures, or associated documentation used in the operation of a computer system.

   f. **Computer System -** A set of related computer equipment, hardware or software.

B. **Data -** A representation of information, knowledge, facts, concepts, or instructions that has been prepared or are being prepared in a formalized manner and have been processed, are being processed, or are intended to be processed in a computer system or computer network. Data may be in any form including computer printouts, magnetic storage media, compact discs, and as stored in the memory of University computers.

C. **Data Custodian** – The individual responsible for the accuracy and institutional responsibility for a set of data.

D. **Electronic Protected Information** - individually identifiable information that is in two states:

   1. Data at rest or maintained in electronic media

2. Data in motion or transmitted by electronic media

E. Electronic Media –

1. ***Storage media***, such as memory devices, including computer hard drives, flash drives, memory sticks, and any other removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card.
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.

F. Enterprise Technology Services (ETS) – formerly Information Systems and Services (ISAS), is the "owner" of the University's *Acceptable Use* policy. Unit policies and protocols are "owned" by the Responsible Officer and the respective office, division, department or other organizational unit. (Refer to 400-001 *Policy on Policies* for more information.)

G. 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.

H. 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.

I. 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.

J. Sensitive Information (Personally Identifiable 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.

K. Technology Resources - Any and all computer or electronic resources that are used in the search, access, acquisition, transmission, storage, retrieval, or dissemination of data.

L. User - Any person authorized to access and use information technology resources at HU. This includes, but is 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.

M. **User Account** - Any logical access on any University computer system that has been specifically established for a particular user. A user account may have a dedicated logical area on one or more University computer systems also associated with it.

V. POLICY PROCEDURES

This policy will be implemented by 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. Maintenance, monitoring, enforcement, and clarification of the *Acceptable Use Policy* will be facilitated by ETS.

A. GENERAL USE AND OWNERSHIP

While network administration 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. A reasonable level of privacy is balanced with the requirement to protect the University from risk.

Employees are responsible for exercising good judgment regarding reasonable personal use. ETS creates policies that govern network, device, or application usage and the enterprise as a whole: all private information (such as Social Security Numbers, protected health information, credit information, passwords, etc.) must be protected from unauthorized disclosure.

ETS recommends that any information that users consider sensitive or vulnerable be encrypted. (See the Appendix for Sensitive Information categories.) For the integrity, confidentiality, and availability of the resources, and security and network maintenance purposes, authorized individuals may monitor equipment, systems and network traffic at any time. The right to audit networks and systems on a periodic basis to ensure compliance with this policy is reserved.

B. GUIDELINES FOR ACCEPTABLE USE

Technology resources are an integral tool in the functioning of the University. All who use these resources must understand that they are primarily for the advancement of the University’s mission and values expressed through its teaching, research, public service, healthcare, business and outreach functions. Use of these resources is permitted only in conformity with these values as expressed in University policy, and in compliance with federal, state and local law.

In addition to this statement of acceptable use, below are specific categories of use, which provide additional guidance.

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. Faculty, staff, students, residents and others with permission 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.

Commercial Use

The use of computing resources for commercial purposes is only permitted under University policy, including University intellectual property policy, by special arrangement with the appropriate official, or as defined in any existing conflict of interest policies. Permitted commercial use must be communicated in writing to ETS, and the policies of this document are still applicable. Any commercial use that is accessible to others must include a disclaimer.

Legal Use

The computing resources may only be used for legal purposes.

Examples of unacceptable and illegal use include, but are not limited to the following:

1. Discrimination or harassment on the basis of race, color, religion, national origin, sex, age, marital status, personal appearance, sexual orientation, familial status, family responsibilities, matriculation, political affiliation, disability, source of income, or place of residence or business.
2. Violation of any University licensing agreement or any copyright or trademark law, including unauthorized copying of copyright-protected material.
3. Libel, slander, defamation, or bullying of another.
4. Destroying or damaging equipment, software or data belonging to the University or any other user.
5. Accessing pornography for purposes other than education or research.
6. Use for illegal or unlawful purposes, including 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).

7. Violating HIPAA, FERPA and other applicable laws as they relate to computing resources and protecting personally identifiable information (Sensitive Information).

Ethical Use

Computing resources should be used in accordance with the ethical standards of the University community. (See *700-001 Social Media* for more information.)

Examples of unethical use, some of which may also have legal consequences, include, but are not limited to, the following:

1. Use of computing resources in ways that unnecessarily impede the computing activities of others, such as randomly initiating interactive electronic communications or e-mail exchanges, overuse of interactive network utilities and similar activities
2. Use of computing resources for private business purposes unrelated to the mission of the University or University life, absent authorization as stated in this policy
3. Academic dishonesty, for example plagiarism or cheating
4. Violation of network usage policies and regulations.

Cooperative Use

Users of the computing resources can facilitate computing at the University in many ways. Collegiality demands the practice of cooperative computing:

1. Regularly deleting unneeded files from one’s accounts.
2. Refraining from any use that overloads or otherwise negatively impacts the performance of the computing resources including, without limitation: overuse of connect time, information storage space, printing facilities or processing capacity.
3. Refraining from use of sounds and visuals which might be disruptive to others.
4. Refraining from irresponsible use of any computing resource.
5. Refraining from unauthorized use of a departmental or individual computing resource.

Political Use

The use of University computing resources (duplication machines, computers, telephones, fax machines, scanner, etc.) by faculty or staff in connection with political campaign activities in support of or in opposition to individual candidates, political parties, or political action committees *is prohibited*.

To the extent that such political activities can be considered a gift, donation, or contribution to a candidate, political party, or political action committee, this policy also applies to students and student organizations. No use which, by inclusion of the University's name, images, symbols or trademark, may tend to convey the impression that Howard University endorses or opposes any candidate, political party or political action committee is permitted, regardless of one's status as a student, faculty member, staff member or other. Nothing in this policy shall be construed to prevent students and student organizations from independently engaging in political or public interest activities.

C. RESPONSIBILITIES OF THE UNIVERSITY

Users are advised that the University does not guarantee the confidentiality or privacy of any information entered into, stored, transmitted or received via University computing resources, except in compliance with local, state, and Federal regulations. There is no expectation of privacy in any information or data entered into, stored, transmitted or received.

The University may access, search, view, retrieve, or print information or data entered into, stored, transmitted or received via computing resources in connection with, the following:

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

In general, requests for disclosure of information entered into, stored, transmitted or received on computing resources will be honored only under one of the following conditions:

1. When approved by the appropriate University official(s) or the head of the department.
2. When authorized by the owners of the information.

3. When required or not prohibited by federal, state or local laws.
4. Where appropriate and possible, the University will provide notice of disclosure to the affected computer user(s).

D. RESPONSIBILITIES OF USERS

1. The user should assign an obscure or complex account password as dictated by the terms of *700-003 Password Security*.

2. No one should share a password with another and should treat the password as his/her own personal signature.

3. Activities under an individual’s own username and password are to be understood as their own activities for which a user is accountable and responsible.

4. Only the person to whom it is assigned may use a University computer account.

5. The computer user should be aware of computer viruses and other destructive computer programs, and take all available precautions against attacks.

6. While the University seeks to provide availability, integrity, and confidentiality of its resources, the user must assume responsibility for invasion of the user’s or another's privacy and for any loss of data.

7. The user is responsible for reporting all possible security concerns or incidents on any University computer, computer system or network to the IT security officer, system administrator or a member of ETS senior management immediately.

E. SECURITY AND PROPRIETARY INFORMATION

The user interface for information contained on Internet/Intranet/Extranet-related systems should be classified as either *Confidential* or *Not Confidential*. Examples of confidential information include, but are not limited to: information and knowledge about Howard University and/or its constituents that are accessible to the user based on his/her position at or relationship to Howard University; University strategies; specifications; vendor lists; research data; or other limited access data. User interfaces for individuals who routinely handle Sensitive Information should be classified as *Confidential*.

Employees should take all necessary steps to prevent unauthorized access to Confidential information.

1. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. System level passwords should be changed quarterly; user level passwords should be changed every six months.

2. All PCs, laptops and workstations should be secured with a password-protected screen-saver with the automatic activation feature set at 10 minutes or less, or by logging-off when the host will be unattended.

3. Use encryption of information in compliance with ETS policies external transmission of Sensitive Information, such as Protected Health Information (PHI) and Social Security numbers.

4. Because information contained on laptop computers is especially vulnerable, special care should be exercised. Transporting, downloading or emailing confidential data without proper and authorized security measures applied is prohibited. Staff should take great caution to protect these devices when traveling, or using them from remote locations.

5. University employees who post to newsgroups should include a disclaimer in their email stating that the opinions expressed are strictly their own, unless posting is in the conduct of University business.

6. All hosts used by the employee that are connected to the Internet/Intranet/Extranet, whether owned by the employee or the University, shall be continually executing ETS approved virus-scanning software with a current virus database

7. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses or other destructive code.

F. UNACCEPTABLE USE

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing University-owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities, which fall into the category of unacceptable use. No list of acceptable uses or prohibited activities can be complete. Below are examples of prohibited activity:

1. Circumventing or attempting to circumvent any system security.
2. Gaining or attempting to gain unauthorized access to any University computer account.
3. Causing overload or otherwise negatively impacting the performance of University computing resources.
4. Sending e-mail under another’s e-mail address (e.g., “spoofing”) for any purpose.

5. For individuals in the workplace, excessive personal use of email, Internet, social media or other non-work related activities on University computing resources.
6. For individuals in the workplace, use of personal email accounts, such as Gmail, Yahoo, AOL, are discouraged as channels of official communication. However, in certain circumstances, such as when the University network is down, personal accounts may be used as a temporary work-around. Personal accounts should not be used to transmit Sensitive Information.
7. Sending or transferring Sensitive Information via unsecure email or other electronic media. Such messages should be encrypted.
8. Sending or collecting chain letters or unsolicited bulk mail messages to the University community or other population.
9. Invading the privacy or confidentiality of any other user including, without limitation, accessing or attempting to access another's account without permission from the account holder or as requested by the Office of General Counsel and/or a written request from the Campus Police Chief.
10. Altering the integrity of any data or information stored in or used by the University community or other population.
11. Harassing or bullying another person, group or organization on any basis.
12. Disrupting or monitoring electronic communications of another without authorization from the Office of General Counsel or a written request from the Campus Police Chief.
13. Preventing another authorized user from that user's authorized access, or otherwise interfering with another's authorized use.
14. Stating or implying University sponsorship or endorsement.
15. Engaging in any use that results in any direct cost to the University.

G. SYSTEM AND NETWORK ACTIVITIES

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or entity protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use.

2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which the University or the end user does not have an active license is strictly prohibited.

3. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.

4. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

5. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.

6. Using a computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.

7. Drug trafficking, sales and/or distribution.

8. Making fraudulent offers of products, items, or services originating from any University account.

9. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.

10. Effecting security, data breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient, or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

11. Port scanning or security scanning is expressly prohibited unless job-related and/or prior notification to ETS Network Services is made.

12. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.

13. Circumventing user authentication or security of any host, network or account.

14. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).

15. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.

16. Providing confidential information, per Section V.E. of this policy, to unauthorized parties.

H. EMAIL AND COMMUNICATIONS ACTIVITIES

These are actions that unacceptable with respect to using the enterprise network for sending and receiving email with any email account:

1. Sending unsolicited email messages, including the sending of “junk mail” or other advertising material to individuals who did not specifically request such material (email spam).
2. Any form of harassment via email, telephone or texting, whether through language, frequency, or size of messages.
3. Unauthorized use, or forging, of email header and other email content.
4. Solicitation of email for any other email address, other than that of the poster’s account, with the intent to harass or to collect replies.
5. Use of unsolicited email originating from networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by or connected via the network.
6. Creating or forwarding “chain letters,” “Ponzi” or other “pyramid” schemes of any type.
7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam)
8. Any personal e-mail account, creation of a personal webpage or a personal collection of electronic material that is accessible by others and suggests affiliation with the University, must include a disclaimer stating: The material located at this site is not endorsed, sponsored or provided by or on behalf of Howard University.

VI. INTERIM POLICIES

There are no interim policies.

VII. SANCTIONS

For students, faculty, staff and recognized organizations, reporting of, discipline for, and sanctions for violations of these policies will be indiscriminate. In addition, the sanctions provided for violating the applicable policy, shall range from temporary or permanent loss of computing privileges, to reporting the violation(s) to administrators of other computing resources and federal, state or local law enforcement authorities. Violations of the legal and ethical use provisions of this policy are serious infractions and shall result in disciplinary actions as allowed by Human Resources, *Student Code of Conduct*, *Social Media* and other pertinent University policies and procedures.

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

www.howard.edu/policy

Other related University policies:

- 700-001 *Social Media*
- 700-003 *Password Security*

Other related Unit policies:

- *Removable Media Policy* (in draft form)
- *Security Incident Policy* (in draft form)

External Resources:

Family Educational and Privacy Rights Act of 1974 (FERPA)
Health Insurance Portability and Accountability Act (HIPAA)
Financial Modernization Act of 1999 (Gramm-Leach –Bliley)

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
- Birth date
- Home phone number and address
- Personal contact information
- Education and training
- Non-salary financial information (such as expense reimbursements, pension information, or fringe benefit value)
- Benefits information
- Health records
- Passwords
- 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 ID Number
- Grades
- Courses taken
- Schedule

- Test scores
- Advising records
- Educational services received
- Disciplinary actions
- Financial aid/grant information
- Student tuition bills
- Payment history

<u>Patient Health and Research</u>

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.)