HOWARD UNIVERSITY POLICY

Policy Number: Series 700: Information and Technology
Policy Title: 700-005 MOBILE DEVICE MANAGEMENT POLICY
Responsible Officer: Chief Operating Officer
Delegated to: Chief Information Officer, Enterprise Technology Services
Responsible Office: Office of the Chief Operating Officer
Delegated to: Enterprise Technology Services
Effective Date: August 14, 2015

I. POLICY STATEMENT

Howard University's ("the University's") network and computing technology provide information, data, and communication services. Mobile devices issued or personally owned, brought and used within the University's network must be in compliance with appropriate security controls and restrictions.

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

II. RATIONALE

This policy defines the responsibilities, guidelines, terms of use and management of University-issued and employee-owned mobile devices. This policy covers devices configured for access to University data, such as personally identifiable information, protected health information, academic research, intellectual property, and financial data.

III. ENTITIES AFFECTED BY THIS POLICY

This policy applies to all Howard University and Howard University Health Sciences employees who wish to access computing resources on any mobile device. The Howard University Hospital (HUH) is not affected by this policy.

IV. DEFINITIONS

A. **Computing Resources** – Computer hardware, software, data and network resources used by the University including applications, intranet web access and University email, calendar, or contacts.

B. **Device Management** – Management, security, and monitoring of all mobile devices that access to University Computing Resources, as described in the University Device Management System.

C. **Encryption** – Process of converting data into an unreadable format that is reversible with the use of a security key or password.

D. **Mobile Device** – Cell phone, smartphone, tablet, or laptop intended to be used to perform University related work activities.

E. **Personal Device** – Piece of electronic equipment, such as a laptop or a mobile phone, which is small, easy to carry and owned by an individual.

F. **Personally Identifiable Information** – Any information that can be used to distinguish one person from another and can be used for de-anonymizing anonymous data.

G. **Protected Health Information -** Any information about health status, provision of health care, or payment for health care that can be linked to a specific individual.

H. **Remote Wipe (Remote Wiping Capability)** – Security feature that allows a system administrator or device owner to send a command to a computing device and delete data.

I. **Users** – Employees, contractors, consultants, temporary workers, and other persons or entities authorized to use approved Mobile Devices to access University Computing Resources.

J. **Jail Broken Devices** – the process of removing hardware restrictions on mobile manufacturers' operating system, on devices running it through the use of software and hardware exploits.

V. POLICY PROCEDURES

A. MOBILE SECURITY STANDARDS

Anyone wishing to connect to University data or network resources must comply with the provisions of this policy.

1. Mobile Device Restrictions and Control

The University requires that mobile devices meets technical security controls and restrictions. All enrolled devices must have:

a) Strong passcodes of at least four digits;
b) Device encryption enabled;
c) Data backup capability;
d) Remote wiping capability; and
e) Follow University official device provisioning method for that model.

2. Accessing Institutional Computing Resources

a) As a prerequisite for accessing University computing resources on a user's personal device, the user must have their device provisioned in compliance with University mobile security standards set forth in the *Network Security Policy*.

b) Once an individual provisions their mobile device, University access and data may be managed and controlled by the University Device Management System.

3. User Modified Devices

User-modified devices (such as "jail-broken" devices and "rooted" devices) pose a risk to the University's computing resources. Therefore, the University may disable or remove access to computing resources for devices that have been so modified.

B. EXPECTATION OF PRIVACY

1. Information Technology Responsibilities

a) Enterprise Technology Service (ETS) requires configuration of the user's mobile device to comply with mobile device restrictions and controls to access University computing resources.
b) ETS may perform a "remote wipe" of data from a user's lost or stolen mobile device. In some situations, ETS may perform a full device wipe upon the user's request or upon termination of employment with the institution. ETS will not wipe any personal data from users' devices without their consent or approval.
c) ETS is responsible for maintaining a list of stipend-designated individuals and providing related operational departments access to that list.

2. User Responsibilities

a) The user will not download or transfer restricted business data, such as PII, PHI, etc., to their mobile device outside of managed and approved mobile computing resources and applications.
b) The user will password-protect the Mobile Device.
c) The user must maintain the original Mobile Device operating system and keep the device current with security patches and updates, as released by the manufacturer.
d) The user agrees not to allow any other person to use his/her mobile device to access any HU or HUH applications or data.
e) The user agrees to delete any restricted business files that may be inadvertently downloaded and stored on the device through the process of viewing email attachments.
f) The user will not download/transfer sensitive business data/documents to any third party service or other computing device not approved for use.
g) The user will be required to implement an encrypted backup of their personal data.

h) The user is responsible for contacting the ETS Help Desk immediately in the event that their Mobile Device is lost or stolen.
i) The user is responsible for contacting the ETS Help Desk immediately if they have replaced their Mobile Device.
j) The user is responsible for all Mobile Device support requirements, including the cost of repairs or replacement.

3. User Responsibilities (When Approved for Mobile Device Stipend)
   a) The user is responsible for paying all monthly/annual fees to the mobile carrier. All mobile charges that the user incurs are the responsibility of the user, regardless whether such charges are for work or personal use of the phone. All monthly/annual fees include, but are not limited to, charges resulting from texts, data plan surcharges, phone calls, GPS navigation, application (app) purchases and use, and early termination fees.
   b) The user receiving a monthly stipend is responsible for notifying ETS immediately when mobile service for an enrolled device is discontinued.

VI. INTERIM POLICIES

There are no interim policies.

VII. SANCTIONS

Individual employees who inappropriately use or misuse the University network and/or consciously compromise protected information shall be subject to disciplinary loss of mobile device network privileges and disciplinary action, up to and including termination of employment. Inappropriate use or misuse of the University network may include, but is not limited to actions that violated federal or state law (i.e., HIPAA or FERPA), and access to websites that contain pornography.

The University reserves the right to temporarily or permanently remove a user account on the network to prevent further unauthorized activity.

Illegal use of the network, intentional deletion or compromise of protected information and theft of services shall be reported to appropriate legal authorities as necessary.

VIII. HYPERLINKS

Howard University Policy website: www.howard.edu/policy
Other related policies:

700-002 *Acceptable Use of University Information Resources, Data and Communication Services Policy*
700-003 *Password Security* and Related *Waiver*
700-004: *Mobile Device Stipend Policy*