HOWARD UNIVERSITY POLICY

Policy Number:	700-003
Policy Title:	HOWARD UNIVERSITY PASSWORD SECURITY
Responsible Officer:	Chief Information Officer
Responsible Office:	Office of the Chief Information Officer
Effective Date:	March 5, 2012

I. POLICY STATEMENT

Members of the Howard University ("the University") community can access the University's various information systems by using passwords, which are an important aspect of computer security. Passwords function as "keys" that enable users to access the University's wide range of services, such as e-mail, PeopleSoft, Banner, BisonWeb, Blackboard, the Virtual Private Network (VPN), and Concur. They serve as the primary means to control access to systems and therefore should be created, used and managed to protect against unauthorized discovery or use. This policy establishes requirements for appropriate password creation and handling to help ensure personal security, and to protect the University's information systems resources.

II. RATIONALE

As a comprehensive research university, it is essential to have networks that are reliable, secure and accessible. As the private part of a user's digital identity, passwords are foundational to University information systems and must therefore be created according to best practices and guarded with utmost care. A poorly chosen password may compromise the University's entire network. The purpose of having a password policy is to ensure a more consistent measure of security for Howard University's systems and the information they contain. The implementation of this policy will better protect the confidential information of all individuals and organizations affiliated, associated, or employed by the University. Additionally, this policy establishes a standard for creating, protecting and managing passwords.

III. ENTITIES AFFECTED BY THIS POLICY

This policy applies to all persons using a Howard University account at any time or location, including students, student assistants, faculty, staff, temporary or volunteer staff, alumni, retirees, and other Howard University affiliates (including contractors) with access to password-protected University resources. This policy affects Howard University and Howard University Hospital.

IV. DEFINITIONS

A. **Account Holder** – any person associated with Howard University with access to password-protected resources. Account holders are held responsible for all activities associated with their accounts.

B. **Help Desk –** the Support-Service Desk administered by Enterprise Technology Services (ETS) to assist clients with information technology issues. The Help Desk is accessible by phone (202) 806-2020 or online at http://help.howard.edu.

C. **User -** every person using a Howard University account at any time or location, including students, faculty, staff, alumni, retirees, volunteers, and other Howard University affiliates (contractors and vendors) with access to password-protected University resources, at Howard University and Howard University Hospital.

D. **Password** - A sequence of alphanumeric and special characters entered in order to gain access to a computer system or information resource.

   a. System-Level Passwords – passwords used by systems administrators to access and maintain enterprise-wide applications and databases (also referred to as the Administrator password).

   b. Production System-Level Passwords – used to distinguish a "live" or presently used application or database instead of a test or development system.

   c. User-Level Passwords – passwords that are used to access individual accounts; email, BisonWeb, PC or Mac machine access, etc.

All system-level and production system-level passwords MUST be communicated to the director responsible for the associated systems. This will ensure that the unit is always able to perform administrative functions in the event of emergencies, personnel transitions, and other such situations.

V. POLICY PROCEDURES

Handling of Passwords in the Workplace

Passwords are an important aspect of computer security and should be chosen carefully. Users shall follow these guidelines in handling passwords to University resources:

A. No passwords are to be spoken, written, e-mailed, hinted at, shared, or in any way known to anyone other than the user involved. This includes supervisors and personal assistants.

B. No passwords are to be shared in order to "cover" for someone absent, unavailable, etc.

C. Passwords are not to be displayed or concealed on a workspace.

D. All system-level passwords must be changed at least on an annual basis.

E. All production system-level passwords must be part of the administered global password management database.

F. All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed every 90 days.

G. All user-level and system-level passwords must conform to the guidelines described below.

General Password Construction Guidelines

Passwords are one of the most commonly used methods to prevent unauthorized access to computers and files. Password hackers are becoming increasingly more sophisticated, and as a result it is recommended that users make use of "Strong Passwords." Strong passwords, when created properly have multiple characteristics. Reference the following list for characteristics of a strong password:

A. Make the password long and complex, but easy for to remember, so it is hard to crack. A minimum of nine (9) characters is required.

B. Three (3) out of four (4) of the following must be used to construct your password:
    a. At least one uppercase letter;
    b. At least one lowercase letter;
    c. A number, or;
    d. A special character (#, @, $, %, etc.).

C. Make a password easy to type quickly. This will make it harder for someone in close proximity to steal the password by looking over your shoulder.

D. It is important to use a password safely by:
    a. Creating different passwords for different accounts and applications so that if one account is breached, all other accounts are not at-risk, too.
    b. Never use your HU password for online shopping sites or free e-mail accounts.
    c. Change passwords regularly, every 90 days.
    d. Do not share passwords with anyone else – once it is out of your control so is all security.
    e. Never enable the *Save Password* option, even if prompted to do so. Pre-saved passwords make it easier for anyone else using your computer to access your accounts.
    f. Never walk away from a shared computer without logging off to ensure that no other users can access accounts via your password.
    g. Do not use sample passwords given on different Web sites.
    h. Do not create passwords based on personal information, such as family names, etc.
    i. Do not reveal a password over the phone to anyone.
    j. Do not reveal a password in an e-mail message.
    k. Do not reveal a password to auditors.

l. Do not talk about a password in front of others.
m. Do not hint at the format of a password (e.g. “my family name”)
n. Do not reveal a password on questionnaires or security forms.
o. Do not share a password with others, including family members.
p. Do not reveal a password to co-workers even if on vacation.

Exception

An exception to this policy is provided below and will be granted on a case-by-case basis:

The account holder/user is a dean, director, vice president or cabinet member and has delegated certain administrative responsibilities to a designee. The account holder/user must submit a *Password Distribution Waiver Request Form* electronically to ETS for review and approval. It is the responsibility of the dean, director, vice president or cabinet member to notify ETS when personnel changes impact this exception. If the designee is separated from the University, the account holder is required to change his/her password(s) immediately.

VI. INTERIM POLICIES

Hackers and other Internet criminals are constantly evolving new strategies for breaking through security measures, so the University must remain informed about current best practices regarding password security. As best practices change, this policy will be updated to better inform and educate University users.

VII. SANCTIONS

Violations of this policy by University employees and students 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 others with permission to use University computing resources should be reported to ETS and will be handled at the discretion of the Administration. Sanctions may include among other things, revocation of use privileges or loss of contract.

VIII. WEBSITE ADDRESS

www.howard.edu/policy

Related Document: *Password Distribution Waiver Request Form*

Related policies: *600-001 Howard University Student Code of Conduct*
700-001 Social Media