

Virginia Commonwealth University Technology Services

Password Standard

Definition:	<i>This standard applies to all users who access the VCU network.</i>
Designation:	Technology Services Standard
Effective Date:	April 19, 2007
Review Frequency:	Annually or as needed
Authority:	VCU Chief Information Officer VCU Security Officer
In Compliance with:	VCU Academic Policy: Security of Electronic Sensitive Information VCU Academic Policy: Information Security Policy UITAC Goals: <i>Infrastructure Goal 3.</i> COV ITRM Information Technology Security Management Standard SEC501-01 VCU Computer and Network Resources Use Policy

Scope:

This standard covers the use of passwords for accessing systems on the VCU network. The eID is the single-sign-on authentication mechanism for most VCU enterprise applications. eID password requirements, which are compatible with Banner, are listed below. Users fall into several categories or groups based on their roles and use of applications at VCU. The requirements for length, composition and complexity are the same for all groups. The requirements for password expiration, uniqueness and the forgotten password self-service feature are specific for each group. The user groups for passwords are defined as:

1. Student – this account is used by individuals who are enrolled as students as their first affiliation.
2. Faculty/Staff – this account is used by individuals who function in the role of faculty or employee
3. INB Banner – this is an account used by individuals who are users of INB (Internet Native Banner)
4. Application Account – this is an account that is used by an application to make a connection to the enterprise directory.
5. Administrative Account – this account is used by system administrators of the enterprise directory.
6. Temporary Guest Account – this is a temporary account that is created for a non-VCU individual

For systems that do not use eID for authentication such as logon access to local area networks and local workstation logons, the password used for logon authentication **must at a minimum** fulfill the requirements for length, composition and complexity for eID passwords listed below.

For privileged access such as administrative logons to servers, the password used for authentication must fulfill the requirements listed below for administrative system access.

The General Requirements section of the standard applies to all users.

Applied Industry Best Practices of:

- National Institute of Standards Technology (NIST)
- Center for Internet Security Consensus Security Benchmarks
- SANS Institute Password Best Practices and Policy Template

Requirements of the Standard

General Requirements

- Passwords are required for all access to systems on the VCU network.

- Blank passwords are not allowed.
- Passwords must comply with the level of access to sensitive information
The principal of least privilege must be followed on public computers, and the local logon accounts should not have administrator privilege.
- Passwords must be kept secret and must not be shared.
- Passwords must not be inserted into email messages or other forms of electronic communication and should not be stored in a file or computer system without encryption.
- Passwords should not be stored using the "Remember Password" feature of applications (e.g., Eudora, Outlook, Netscape Messenger).

Requirements for eID Passwords

- **Length:** Passwords must be from 7 to 12 characters long
- **Composition and Complexity:** Passwords must include
 - At least one upper case letter and one lower case letter and no special characters (e.g., #, >, %, @, *, etc). (Banner will not allow special characters).
 - At least one numeric that is not at the end or the beginning of the password.
- **Expiration:** eID Password expiration depends on user groups as follows:
 - **Student** – expiration is every 365 days
 - **Faculty/Staff** – expiration is every 365 days
 - **INB Banner** – passwords expire every 90 days
 - **Application Accounts** – passwords do not expire and cannot be changed by user
 - **Administrative Accounts** – passwords expire based on system requirement
 - **Guest Accounts** – passwords expire within 90 days or less
- **Uniqueness:** eID Password cannot be re-used:
 - **Student** – must be unique; last 4 are kept in history
 - **Faculty/Staff** – must be unique; last 4 are kept in history
 - **INB Banner** – must be unique indefinitely
 - **Application Accounts** – must be unique indefinitely
 - **Administrative Accounts** – must be unique indefinitely
 - **Guest Accounts** – N/A
- **Forgotten Password Challenge/Response:**
 - **Student** – must set answers to 5 administrator-defined challenge questions
 - **Faculty/Staff** - must set answers to 5 administrator-defined challenge questions

- **INB Banner** – can set answers to 2 user-defined challenge questions
- **Application Accounts** – no password self-service feature
- **Administrative Accounts** – no password self-service feature
- **Guest Accounts** – no password self-service feature

Requirements for Administrative Passwords

- Strong Passwords for administrative accounts should contain the following:
 - Include both upper and lower case characters (e.g., a-z, A-Z)
 - Have digits and special characters as well as letters (e.g., 0-9, !@#\$%^&*()_+|~-=\`{}[]:;'<>?,./)
 - For Windows administrator accounts, there must be a method for preventing LM hashes being stored, such as the use of the NoLMHash key or the use of a complex password/pass phrase greater than 14 characters.
 - Have at least eight alphanumeric characters (greater than 14 for Windows administrators) and be a pass phrase (e.g., Ohmy1stubbedmyt0e).
 - Not be a word in any language, slang, dialect or jargon
- The best practice is that all system-level passwords (e.g., root, system admin, application administration accounts, etc.) must be changed on at least a quarterly basis; however, where such practice is impractical due to support issues, the administrative password should be changed as frequently as practical.
- Administrative passwords must be changed whenever there is a change in the technical staff that has administrative account access and whenever there is a suspicion of possible system compromise.
- Passwords for administrative or system level accounts should be unique and not used as passwords for other accounts the administrator may have on the system.
- Where SNMP is used, the community strings must be defined as something other than the standard defaults of "public," "private" and "system" and must be different from the passwords used to log in interactively. A keyed hash must be used where available (e.g., SNMPv2).

Implementation Guidelines

See password information and recommendations at this site:
<http://www.ts.vcu.edu/faq/security/strongpasswords>

Enforcement

Violation of this standard could result in loss of access to applications or to the VCU network or personnel disciplinary actions.

Exceptions

Requests for exceptions to the requirements of this standard should be made in writing (by hard copy or email) to the VCU Chief Information Officer.

Revision History: