**PURPOSE:**

The University of Richmond is committed to a secure information technology environment in support of its mission. In today's environment the need for a strong password policy is greater than ever. Many systems at the University require the use of passwords including but not limited to e-mail, academic and administrative applications, computing labs, box, and VPN.

**SCOPE:**

This policy applies to the University of Richmond and all of its Affiliates. As used in this policy, the term “Affiliates” means organizations or entities in which the University owns a controlling interest or has the right to elect the majority of the entity’s governing board.

**INDEX:**

IRM-4001.1......Policy Statement
IRM-4001.2......Applicable Regulations and Accreditation Standards

**POLICY STATEMENT:**

*IRM-4001.1 – Policy*

**Password Rules:**

- Your login ID and password authenticate you as an authorized user of the University of Richmond's computing environment. A strong password is key to the University's overall systems security. You must protect your files and University resources by choosing a good password and protecting it.

- You are responsible for safeguarding the passwords for your computing accounts. Passwords must not be shared or disclosed to anyone including friends or family. If another person learns your password,
that individual has the ability to access your e-mail, your personal files, and your online network identity, and accounts. A knowledgeable person could use your account to attempt to gain unauthorized access to other networked resources, putting them at risk. No one should be given your password—not even someone from Information Services. If you become aware that someone else has learned your password you should change it immediately.

- Hackers gain access to systems by "cracking" accounts. They typically accomplish this through the use of automated processes to discover account IDs and passwords. Using a dictionary word or your account ID for a password puts your system (and the University's systems) at higher risk of attack by hackers.

- It is strongly recommended that you change all your passwords regularly, at least once per year.

- Do not use the password that you choose for your University of Richmond accounts with other off-campus services such as Facebook, Twitter, LinkedIn, Google and Yahoo. This is to protect your Richmond accounts in case those services are breached or in case your service provider does not encrypt passwords during the authentication process. You must change your password immediately if you notice unusual activity on your system or account. If you suspect that someone is accessing computing resources using your identity, please contact the Help Desk at (804) 287-6400 or report it to the Information Services Security Administrator at infosec@richmond.edu.

How to Choose a Strong Password

One of the goals of this policy is to create a strong password that you will remember, but unpredictable for others. As such, your password is less likely to be guessed and your account hacked into. Rules for length and complexity of passwords are outlined below.

**Password Length**

1) Minimum password length: 16 characters
2) Maximum password length: 30 characters

**Password Complexity**

3) Characters limited to: a-z, A-Z, 0-9 and [ ] & * @ ! % ? = ~ #
4) Password must contain at least one lowercase letter, one uppercase letter, and one number.
5) Password must contain at least 5 unique characters and no more than four characters can be in a “sequence”. For example a password of “A1a1a1a1a1a1a1a1” or passwords containing “aaaaa”, “abede”, “55555”, “12345”, “54321”, etc. are not allowed.
6) Disallow usage of the following personal information embedded in your password:
   - Netid
   - Name (first, middle, or last)
   - Birth year (YYYY)

   Example: “presidentAlincoln1809” not allowed (if you are Abe Lincoln).

**Password Maintenance**

7) Passwords must be changed only once every 360-370 days.
8) Successive passwords must differ by at least 3 characters.
9) Passwords that have been used within the last 18 months cannot be re-used.
10) An uppercase character ('C') is considered different from a lowercase character ('c'), except when comparing successive passwords, in which case they are considered the same (e.g., can’t change password from 'Cat' to 'cAT').

**If You Forget Your Password**

- Contact the Help Desk at (804) 287-6400 (you will be asked to provide information to verify your identity) or visit the Help Desk in Jepson Hall G-19 (with your picture ID) to have your password reset.
- In addition to the traditional method of resetting a forgotten network password by calling or visiting the IS HelpDesk, you are be able to register a 10-digit phone number to which a PIN will be sent (via text) that can be used to reset your password. Your phone must be capable of receiving text messages.

**IRM-4001.2 – Applicable Regulations and Accreditation Standards**

SACSCOC Principles of Accreditation 10.6 (Distance and Correspondence Education)

**Related Policies:**

**Policy Background:**

Policy approved July 28, 2005  
Revised August 5, 2008  
Revised for password length and complexity effective October 30, 2013

**Policy Contacts:**

Vice President for Information Services and Chief Information Officer  
Director of Information Security