UNIVERSITY OF RICHMOND

Policy Manual

Policy #:	IRM-4001	**Policy Title:**	Password Policy
Effective:	04/01/2020	**Responsible Office:**	Information Services
Date Approved:	04/01/2020	**Approval:**	Vice President for Information Services and Chief Information Officer
Replaces Policy Dated:	07/28/2005	**Responsible University Official:**	Vice President for Information Services and Chief Information Officer

PURPOSE:

The University of Richmond is committed to a secure information technology environment in support of its mission. Many systems at the University require the use of passwords including but not limited to email, academic and administrative applications, computing labs, Box®, and networks. In today's digital environment, the need for a strong password policy is greater than ever. This policy defines the requirements for creation of strong passwords and protection of those passwords.

SCOPE:

This policy applies to current faculty, staff, and student accounts that grant access to information systems, data, or networks owned or managed by the University of Richmond. This also includes those who are responsible for approving access as well.

INDEX:

IRM-4001.1.....Definitions

IRM-4001.2…...Policy Statement

IRM-4001.3…...Applicable Regulations and Accreditation Standards

POLICY STATEMENT:

IRM-4001.1 – Definitions

Affiliate – An organization or entity in which the University owns a controlling interest or has the right to elect the majority of the entity's governing board.

User – Any individual, including but not limited to faculty, student, staff, contractors, and visitors who has access and uses University information resources, systems, or data.

IRM-4001.2 – Policy Statement

The University NetID and password authenticates a user and grants authorized access to the University of Richmond's computing environment. A strong password or passphrase is key to the University's overall systems security. Users must protect their files and University resources by choosing a strong password and safeguarding it.

- Users are responsible for safeguarding their passwords to computing resources. Passwords must not be shared or disclosed to anyone including coworkers, vendors, friends, or family. If another person learns your password, that individual has the ability to access your e-mail, personal files, online network identity, and accounts. An attacker could use your account to attempt to gain unauthorized access to other networked resources, putting the University at risk. Never give your password to anyone—not even someone in Information Services.

- One method hackers use to gain access to systems is 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 account and the University's systems at higher risk of attack by hackers.

- University account passwords must be changed annually. It is strongly recommended that you change all your passwords regularly, at least once per year.

- Do not use the password associated with University of Richmond accounts for external accounts and services; such as social media, streaming platforms, shopping, etc. This protects Richmond accounts from compromise in the event such external services are breached or the service provider does not encrypt passwords during the authentication process.

- If you notice unusual activity on your account or suspect someone has learned your password, change the password immediately and notify the Help Desk or Information Security. 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 Director Information Security at abuse@richmond.edu.

How to Choose a Strong Password

One of the goals of this policy is to create a strong password or passphrase that is easy for a user to remember, but difficult for others to guess, making it less likely for an account to be hacked. 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", "abcde", "55555", "12345", "54321", etc. are not allowed.
6) Usage is disallowed for 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 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').

Reset 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 mobile phone number in University Network Account Management 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-4001.3 – Applicable Regulations and Accreditation Standards

A. Red Flags Rule of the Fair and Accurate Credit Transaction Act of 2003 (FACT Act), Public Law 108-159, Section 114
B. Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99)
C. Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191
D. Payment Card Industry Data Security Standard (PCI DSS)
E. SACSCOC *Principles of Accreditation* 10.6 (Distance and Correspondence Education)

RELATED POLICIES:

A. Information Security Policy
B. Acceptable Use Policy
C. Data Security Policy
D. Policy for Payment Card Acceptance and Security

POLICY BACKGROUND:

Policy approved July 28, 2005
Revised August 5, 2008
Revised for password length and complexity effective October 30, 2013
Revised policy to add Definitions; updated the Scope; modified the Policy Statement for clarity added additional regulations and standards; and added Related Policies December 2019
Revised policy reviewed by President’s Cabinet on March 2, 2020; approved by VP & Chief Information Officer on April 1, 2020

POLICY CONTACTS:

Vice President for Information Services and Chief Information Officer

Director of Information Security