

Security Standard – RIT User Account Passwords

1.0 Purpose

The intent of this standard is to make passwords throughout RIT more secure. Weak passwords can be “guessed” or “cracked” allowing unauthorized access that can result in identity crimes, extortion, or damage to RIT’s reputation through the disclosure of sensitive or private information. This is becoming increasingly important because password cracking software is freely available and computer worms and other forms of malicious code now use password attacks to spread.

2.0 Scope

This applies to access control on RIT password protected computing devices, applications, and web pages. It does not apply to RIT systems using Personal Identification Numbers (PINs) such as voicemail. It does not apply to systems service accounts.

3.0 Audience

This standard applies to all users of computing and networked resources owned or leased by RIT, including but not limited to all students, faculty, and staff.

4.0 Minimum Standard

Passwords for the accounts of users and administrators on RIT computing and networked resources must:

- Be at least 8 characters long
- Contain both upper and lower case letters and at least one number or symbol (placed in the middle – not at the beginning or end of the password)
- Be changed *at least* every 120 days
- Not contain your username
- Not be reused (repeated) for at least 6 changes of password

Note: Additional security precautions for choosing and managing passwords can be found at: http://security.rit.edu/bestpractice/securepassword_bp.pdf

5.0 Roles and Responsibilities

This section identifies the roles and responsibilities for implementation and compliance.

- **Information Security Officer** — issues security standards based on threats and the needs of the Institute for protection. The ISO champions implementation efforts, offers acceptable alternatives, and provides exceptions as appropriate. The staff of the Information Security Office provides communication and training materials as appropriate.

- **Information Trustee (VP or Provost)** — comprehends the risks associated with the security standard and provides direction to all students, faculty, and staff within his or her domain to ensure full compliance with the *Minimum Standard* and wherever possible the associated *Best Practices*. In a case of non-compliance, the Information Trustee must agree to a plan that adequately manages the risks until compliance is achieved.
- **End-User** — ensures that all passwords for accounts on computing and networked resources owned or leased by the Institute meet the minimum standard (above).

6.0 Exception Process

If any of the *Minimum Standards* contained within this document can not be met, an Exception Process must be initiated that includes reporting the non-compliance to the Information Security Office with a date for compliance and a plan for risk management until the standard can be met. For more, see:

<http://security.rit.edu/process/exceptions.pdf>

7.0 Related RIT Policies, Procedures, Best Practices and Applicable Laws (not all inclusive)

- RIT's Code of Conduct for Computer and Network Use (C10.0)
<http://www.rit.edu/computerconduct>
- RIT's Information Security Exception Process
<http://security.rit.edu/process/exceptions.pdf>
- Best Practices — RIT Account Passwords
http://security.rit.edu/bestpractice/securepassword_bp.pdf

Jim Moore, Information Security Officer, CISSP, IAM

Date Issued: June 21, 2004

Next Scheduled Review Date: January 21, 2005

For a list of the Contributors and the Revision History: <http://security.rit.edu/standard/PasswordStandardrevhist.pdf>