Security Standard for Authentication Service Providers: RIT 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. It does not apply to RIT systems using Personal Identification Numbers (PINs) such as voicemail; service accounts, applications, or web pages.

3.0 Audience

This standard applies only to system and network administrators that provide authentication services on networked resources owned or leased by RIT and its affiliates.

4.0 Minimum Standard (for authentication providers only)

Systems must be able to verify that the passwords for the accounts of users and administrators on RIT computing and networked resources:

- Are at least 8 characters long
- Contain both upper and lower case letters
- Contain at least one number or symbol
- Are changed *at least* every 120 days

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.

- **Authentication Provider —** responsible for ensuring that:
  - Functionality in existing software applications is enabled and tested to meet this minimum standard no later than **August 29, 2004**.
  - All systems are configured to support the minimum standard no later than **June 30, 2005** or an alternate plan for risk management is provided to their Information Trustee in accordance with the Exception Process by **June 30, 2005**.

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