Password

Policy IT004
Volume 10, Information Technology
Responsible Administrator: Vice President for Information Technology and CIO
Responsible Office: Office of Information Technology
Issued: April 2006
Last Updated: November 2016

Policy Statement

The Fashion Institute of Technology ("FIT" or "the college") is committed to a secure information technology environment in support of its mission. As passwords are a vital component of system security, this policy was instituted to establish a standard for the creation of strong passwords, the protection of those passwords, and the frequency of changing passwords. This policy sets the minimum threshold for passwords that protect the privacy of FIT academic, business, and research information. This policy applies to all information systems at FIT.

Reason for the Policy

This policy is implemented for the following reasons:

- To safeguard and provide security to institutional, professional, and personal data and information by controlling access to the college's electronic computing resources and the network on which they are managed and stored;
- To reduce the potential possibility of electronic identity fraud on campus; and
- To comply with https://www.suny.edu/sunypp/docs/589.pdf.

Who is Responsible for this Policy

- Office of Information Technology

Who is Affected by this Policy

- All persons who are provided an account on the college's network or systems, including employees, guests, contractors, partners, and suppliers.

Definitions

- **Authentication**: A security method used to verify the identity of a user and authorize access to a system or network.

- **Password**: A sequence of characters that is used to authenticate a user to a file, computer, network, or other device. Also known as a passphrase or passcode.

Principles

- **Passwords**
  Passwords are the frontline of protection for user accounts that provide access to safeguarded and protected data and information created by or entrusted to FIT. A structured approach to periodically changing passwords helps protect FIT user accounts from unauthorized access. For this reason, all persons accessing FIT information technology resources must take appropriate steps to create and safeguard their passwords. Most important, this policy helps users understand why strong passwords are a necessity, and thereby, assists them in creating passwords that are both reasonably useable and exceptionally secure.

  A strong password is one that is not easily guessed. It is normally constructed of a sequence of characters, numbers, and special characters, depending on the capabilities of the information technology resources. Typically, the longer the password, the stronger it is. It should never be a name, dictionary word in any language, an acronym, a proper name, only a number, or be linked to any personal information such as a birth date or social security number. It should not be shared with anyone else.

  IT will not distribute passwords without proper identification. You immediately must change the password you are given.

- **Types of Passwords**
  - **Email Account Passwords**
    Email account users may not post or share passwords or other personal authentication credentials that they may have for any account. Users must always use secure passwords when changing their email passwords. To maintain the security of all FIT users' accounts and files, users must change their account passwords at least every 120 days, and their new password cannot be the same as any of the four previous passwords.

  - **Network Account Passwords**
    Network Account Passwords are given to users with access to the FIT internal network and the systems on it. For access to the FIT network, passwords must be at least eight alphanumeric characters long and must contain at least one capital letter, one lowercase letter, and one number. To maintain the security of all FIT users' accounts and files, users must change their account passwords at least every 120 days, and their new password cannot be the same as any of the four previous passwords.

  - **Privileged Account Passwords**
    Privileged Accounts are accounts that are used only by the Office of Information Technology technical staff to access the electronic computing system, hardware, and applications within and outside of the IT Data Center. These passwords must be at least eight characters and include at least one special character or number. These passwords must be changed at least once every 30 days.

  - **Generic Account Passwords**
    Intra-departmental generic accounts are strongly discouraged and should never be created for routine individual communication. However, generic accounts are necessary

for important broadcast communication to the FIT community. Specific exceptions must be approved by the Chief Information Security Officer. Generic accounts may also be created for one-time or short-term special events such as Museum exhibitions, fashion displays, or pageants and shows. Generic accounts that are created for such circumstances must be cancelled immediately at the conclusion of such an event. For access to generic accounts, the password must be at least eight characters and must contain one lowercase letter, one upper case letter, and one number. These passwords must be changed at least once every 120 days.

- **Password Account Exclusions**
  Machine-to-machine passwords, such as those used to communicate between tiers of an application, are excluded from this policy.

Responsibilities

N/A

Procedures

For Password and Accounts procedures, please connect to the https://it.fitnyc.edu

- **Incident Reporting and Enforcement**
  - **Incident Reporting**
    Since a single compromised password can have a catastrophic impact on network security, it is the user's responsibility to immediately report any suspicious activity involving their passwords to their supervisor. Any request for passwords over the phone or email, whether the request came from organization personnel or not, should be expediently reported. When a password is suspected to have been compromised, the IT Help Desk will request that the user, or users, change all of their passwords immediately.

  - **Enforcement**
    Users found to have violated this policy will be required to immediately change their passwords. Accounts for which required password changes are not performed will be locked. In addition, anyone who violates this policy resulting in unauthorized access, disclosure, alteration, or destruction of college data, may be subject to appropriate disciplinary action.

Violations

N/A

Related Policies

- Computer and Network Use
- Email
- Network Access and Security

Related Documents

- How to Change Your FIT Password
- Confidentiality Practices and Protections in New York State, Appendix F (Page7)

Contacts

- **Office of the Vice President for Information Technology and CIO**
  Information Technology
  (212) 217-3400

- **Chief Information Security Officer (CISO)**
  Information Technology
  (212) 217-3400