UNIVERSITY OF NEW HAVEN

Policies and Procedures

Policy Title: Office of Information Technology Password Policy

Policy No.: 7005 Rev.: 1
Effective Date: Oct. 27, 2009
Last Revision: Oct. 21, 2015

Responsible Office: Office of Information Technology
Responsible Official: Associate Vice President for Technology & CIO

Contents

Scope

This policy applies to all employees of University of New Haven who have or are responsible for a computer account, or any form of access that supports or requires a password, on any system that resides at any University of New Haven facility, has access to the University of New Haven network, or stores any non-public University of New Haven information.

Policy Statement

This policy instructs individuals affiliated with The University of New Haven on the use of personal electronic credentials and promotes security, accountability, and appropriate levels of confidentiality in the assignment and use of these personal credentials.

Reason for the Policy

Passwords are a critical part of information and network security. Passwords serve to protect user accounts, but a poorly chosen password, if compromised, could put the entire network at risk. As a result, all employees of the University of New Haven are required to take appropriate steps to ensure that they create strong, secure passwords and keep them safeguarded at all times. The purpose of this policy is to set a standard for creating, protecting, and changing passwords such that they are strong, secure, and protected.

Definitions

Network
A group of two or more computer systems linked together.

OIT
Office of Information Technology.

Internet
A global system of interconnected computer networks that use the standardized Internet Protocol Suite (TCP/IP) to serve billions of users worldwide.

IPsec Secure Virtual Private Network
Provides secure network access to the University's infrastructure from outside the network.

Policy Sections

7005.1 General Policy

- Passwords should be changed every 90 days.
- Old passwords should not be re-used for a period of 6 months.
- All passwords must conform to the guidelines outlined below.

- When creating passwords for users, OIT will notify the user in a separate email from that containing the user's login information.

7005.2 Password Construction Guidelines

Passwords are used to access any number of university systems, including the network, e-mail, the Web, and voicemail. Poor, weak passwords are easily cracked, and put the entire system at risk. Therefore, strong passwords are required. Try to create a password that is also easy to remember.

1. Passwords should not be based on well-known or easily accessible personal information.
2. Passwords must contain at least 8 characters.
3. Passwords must contain at least 1 uppercase letters (e.g. N) and 1 lowercase letters (e.g. t).
4. Passwords must contain at least 1 numerical character (e.g. 5).
5. Passwords must contain at least 1 special characters (e.g. $). The special character @ may not be used.
6. A new password must contain at least 3 characters that are different than those found in the old password which it is replacing.
7. Passwords must not be based on a users' personal information or that of his or her friends, family members, or pets. Personal information includes logon I.D., name, birthday, address, phone number, social security number, or any permutations thereof.
8. Passwords must not be words that can be found in a standard dictionary (English or foreign) or are publicly known slang or jargon.
9. Passwords must not be based on publicly known fictional characters from books, films, etc.
10. Passwords must not be based on the university's name or geographic location.

7005.3 Password Protection Guidelines

1. Passwords should be treated as confidential information. **No employee is to give, tell, or hint at their password to another person, including OIT staff, administrators, superiors, other co-workers, friends, and family members, under any circumstances**.

2. If someone demands your password, refer them to this policy or have them contact the OIT Department.

3. Passwords are not to be transmitted electronically over the unprotected Internet, such as via e-mail. However, passwords may be used to gain remote access to university resources via the university's IPSec Secure Virtual Private Network or SSL-protected Web site.

4. No employee is to keep an unsecured written record of his or her passwords, either on paper or in an electronic file. If it proves necessarily to keep a record of a password, then it must be kept in a controlled access safe if in hardcopy form or in an encrypted file if in electronic form.

5. Do not use the "Remember Password" feature of applications.

6. Passwords used to gain access to university systems should not be used as passwords to access non-university accounts or information.

7. If possible, don't use the same password to access multiple university systems.

8. If an employee either knows or suspects that his/her password has been compromised, it must be reported to the OIT department and the password changed immediately.

9. The OIT may attempt to crack or guess users' passwords as part of its ongoing security vulnerability auditing process. If a password is cracked or guessed during one of these audits, the user will be required to change his or her password immediately.

7005.4 Enforcement

Any employee who is found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.