# Password Policy

## Purpose

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 USEK employees 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 so that they are strong, secure, and protected.

## Scope

This policy applies to all USEK employees 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 USEK facility, has access to the USEK network, or stores any non-public USEK information.

## Policy

### General

1. Old passwords cannot be re-used until the user has changed his/her password three times.

2. All passwords must conform to the guidelines outlined below.

### Password Construction Guidelines

Passwords are used to access any number of company systems, including the network, e-mail, 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 5 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 3 different types of characters (e.g. L_123).

6. A new password must contain, at most, 3 characters from 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, and so on.

10. Passwords must not be based on the company's name or geographic location.

## Password Protection Guidelines

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

2. If someone demands your password, refer them to this policy or have them contact the IT 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 company resources via the company's IPsec-secured 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 necessary 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 USEK systems should not be used as passwords to access non-company accounts or information.

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

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

9. The IT Department 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.

## Enforcement

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

**Name (Printed):** _____

**Name (Signed):** _____

**Today's Date:** _____