COMPUTER PASSWORDS POLICY

1.0 PURPOSE

This policy describes the requirements for acceptable password selection and maintenance to maximize security of the password and minimize its misuse or theft.

Passwords are the most frequently utilized form of authentication for accessing computer resources. The proliferation of automated password-cracking programs and the activity of malicious hackers and spammers exponentially increase security risks when using weak passwords.

Therefore, password use must adhere to the policy statement found below.

2.0 SCOPE

This policy applies to anyone (employees, students, interns, contractors, etc...) accessing or utilizing the network, computers, or data. This use may include, but is not limited to, the following: personal computers, laptops, district-issued cell phones, and hand-held form factor computing devices (e.g., PDAs, USB memory keys, electronic organizers), as well as electronic services, systems and servers. This policy covers departmental resources as well as resources managed centrally.

3.0 POLICY

All passwords (e.g., email, web, desktop computer, etc.) should be strong passwords and follow the standards listed in this policy. In general, a password's strength will increase with length, complexity and frequency of changes.

Greater risks require a heightened level of protection. High risk systems include but are not limited to systems that provide access to critical or sensitive information, controlled access to shared data, a system or application with weaker security, and administrator accounts that maintain the access of other accounts or provide access to a security infrastructure.

All employees, interns, and contractors are expected to set a good example through a consistent practice of sound security procedures.

1. **All passwords must meet the following minimum standards:**
    a. Be at least eight alphanumeric characters long.
    b. Contain at least 1 digit or punctuation character as well as letters (e.g., 0-9, ~`!@#$%()_-'{.})
    c. Contain both upper and lower case characters (e.g., a-z, A-Z).
    d. Not be a word in any dictionary, language, slang, dialect, jargon, etc.
    e. Not be based solely on easily guessed personal information, names of family members, pets, etc.

2. To help prevent identity theft, personal or fiscally useful information such as Social Security or credit card numbers must *never* be used as a user ID or a password.

3. All passwords are to be treated as sensitive information and should therefore never be written down or stored on-line unless adequately secured. ***NOTE:*** *Do not use the password storage feature offered on Windows or other operating systems.*

4. Passwords should not be inserted into email messages or other forms of electronic communication without encryption.

5. The same password should not be used for external or personal access needs (e.g., online banking, personal email, benefits, etc.).

6. Passwords must be changed every three months, or sooner, and must meet complexity requirements.

7. Individual passwords should not be shared with anyone, including administrative assistants or IT administrators. Shared passwords used to protect network devices, shared folders or files require a designated individual to be responsible for the maintenance of those passwords, and that person will ensure that only appropriately authorized employees have access to the passwords.

8. If a password is suspected to have been compromised, it should be changed immediately and the incident reported to the IT department immediately.

3.1 DESKTOP AND USER-LEVEL PASSWORDS

In addition to the general password guidelines listed above, the following apply to desktop and user-level passwords, except where technically and/or administratively infeasible:

1. These passwords must be changed at least every three months.
2. Attempts to guess a password will be automatically limited. Account access will be locked for a minimum of thirty minutes after a set number of failed attempts, unless an administrator intercedes.
3. Failed attempts will be logged. Logs will be retained for a minimum of 30 days. Administrators should regularly inspect these logs and any irregularities or compromises should be immediately reported to the IT department and management.
4. Password cracking or guessing may be performed on a periodic or random basis with the cooperation and support from the appropriate system administrator. If a password is guessed or cracked during one of these scans, the password owner will be required to change it immediately.

3.2 ADMINISTRATOR-LEVEL PASSWORDS

In addition to the general password standards listed above, the following apply to administrator-level passwords, except where technically and/or administratively infeasible:

1. Passwords for servers, routers, firewalls and other security devices must be changed as personnel changes occur.
2. If an account or password is suspected to have been compromised, the incident must be reported to IT and management; potentially affected passwords must be changed immediately.
3. Attempts to guess a password will be automatically limited. Access will be locked for a minimum of thirty minutes after a set number of failed attempts, unless an administrator intercedes.
4. Uniform responses will be provided for failed attempts, producing simple error messages such as "Access denied". A standard response minimizes clues that could result from hacker attacks.
5. Failed attempts will be logged. Logs will be retained for a minimum of 30 days. Administrators should regularly inspect these logs and any irregularities or compromises should be immediately reported to the IT department and management.
6. Password cracking or guessing may be performed on a periodic or random basis with the cooperation and support from the appropriate system administrator. If a password is guessed or cracked during one of these scans, the password owner will be required to change it immediately.

Administrator-level passwords may also be called “enable”, “root”, “admin”, “administrator”, etc…

4.0 COMMON PASSWORD ATTACKS/ CRACKS

Password Guessing

Password guessing involves entering common passwords either manually or through programmed scripts. There are many programs available that will cycle through imported lists of users and passwords and these can be large or small depending on the level of knowledge that user has. Password guessing is usually ineffective because it is a laborious process. In the time it takes to guess a password an attack may be detected and the account locked out.

Dictionary Attack

Dictionary attack is a general threat to all passwords. Depending on the system, the password, and the skills of the attacker, such an attack can be completed in days, hours, or perhaps only a few seconds.

The term dictionary attack refers to finding passwords in a specific list, such as an English dictionary. Dictionary attacks run entire dictionaries through the encryption process, looking for matches. They are a simplistic, yet very effective, approach to finding out who's used common words like "password" or "guest" as their account passwords.

A password database should always be kept secret and secure to prevent a dictionary attack on the data. Obsolete password protection methods also permit dictionary attack by someone who eavesdrops on the network. Strong methods prevent this.

Brute-force attacks

One of the most common password attacks is the simple brute force dictionary attack. An attacker who obtains some sensitive password-derived data, such as hashed-password data, performs a series of computations using every possible guess for the password. Since passwords are typically small by cryptographic standards, the password can often be determined by brute-force. Today, a brute-force approach can compute likely passwords, such as all five-letter combinations, "on-the-fly" instead of using a pre-built list as in a dictionary attack.

Certain passwords are stored in the Windows NT SAM and Active Directory after being passed through a one-way hash algorithm. This type of algorithm is not reversible. Therefore, the only way to tell if you have the right password is to run it through the same one-way hash algorithm and compare the results.

Social-Engineering Attacks

These attacks depend on manipulation. An attacker uses a mix of persuasive skills and statements such as, "I can't secure this system without your password." They may also make claims of authority and misdirection such as, "I'm calling from the IT helpdesk," to fool users into disclosing their passwords. It's hard to put technical solutions in place to stop these attacks.

Network Snooping

Network "sniffers" allow attackers to see network traffic in real time. From this traffic, they can pluck out interesting data, including poorly secured passwords. The good news is that using stronger security protocols like IPSec and Kerberos protect the valuable data by encrypting it so the sniffer only records unintelligible data.

Trojan horses

Like the name implies, a Trojan horse is a seemingly innocuous piece of software that the user is tricked into running. Once the software has been run, it can attack the network in a variety of ways in the user's context. One of the many things it can do is watch the user's key strokes and send them to a third party. For example, a Trojan can capture a user's password when they type it in to authenticate to a non-domain resource.

5.0 POOR PASSWORD CHARACTERISTICS

- The password contains fewer than eight characters
- The password is a word found in a dictionary (English or foreign)
- The password is common usage words such as:
- Names of family, pets, friends, co-workers, fantasy characters, etc.
- Computer terms and names, commands, sites, companies, hardware, software, etc.
- Words including any part of your organization or department name, city, state, zip, or any derivation.
- Birthdays and other personal information such as address and phone numbers.
- Word or numbers patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
- Any of the above spelled backwards.
- Any of the above preceded or followed by digit (e.g., secret1, 1secret)
  Note: These passwords are easy to crack.

6.0 STRATEGIES FOR CHOOSING A GOOD PASSWORD

- **Use lines from a childhood verse**
  Verse Line: Yankee Doodle went to town
  Password: YDwto#town

- **Pick letters from a phrase that's meaningful to you**
  Pass Phrase: Do you know the way to San Jose?
  Password: D!Y!KtwTSJ?

- **City Expression interspersed with street address**
  Chicago is my kind of town
  Password: C1i2mY1K5o6t

  Note: You shouldn't use any of the passwords used as examples in this document. Treat these examples as guidelines only.

7.0 PASSWORD PROTECTION PRACTICES

- Don’t talk about passwords
- Don’t reveal a password over the phone to ANYONE*
- Don’t reveal a password in an email message unless encrypted*
- Don’t reveal a password to the boss*
- Don’t hint at the format of the password(e.g., “my family name”)
- Don’t reveal a password on questionnaires or security forms
- Don’t share passwords with family members or friends
- Don’t reveal passwords to co-workers at anytime*
- Do not use the “Remember Password” feature of applications, websites or operating systems
- Do not write passwords down and store them outside of a securely locked cabinet or safe
- Do not store passwords in a file on ANY computer system (including Palm Pilots or similar devices) without encryption

  If someone demands a password, refer them to this document or have them call someone in the IT Department

**unless previously authorized by the IT department*

REVISION HISTORY

Release No.	Date	Revision Description

REVIEW SCHEDULE
None

OWNER
CIO

DELEGATED OWNER

Network Manager