Idaho Department of Transportation
Enterprise Technology Services

ITD PASSWORD STANDARD

OVERVIEW

Secure accounts and passwords are a vital requirement that provides for sound information and system integrity throughout ITD. A network account with an ineffective password may result in the compromise of the department's critical information, or unauthorized access to a major business system. All ITD employees including contractors, vendors, interns or temporary employees, who have been granted access to the ITD network, and its underlying information systems, are responsible for taking the appropriate steps, as described below, in order to properly and effectively manage their passwords.

The purpose of this standard is to establish rules and guidelines for the creation of effective passwords, the protection of those passwords and to establish the frequency of change. Individuals shall be granted access only to those information systems and repositories necessary to perform their official duties.

SCOPE

The scope of this document includes all personnel who have, or who are responsible for an ITD network account allowing them to gain access to the ITD network. This standard also applies to system level network access in addition to normal user accounts.

GENERAL PASSWORD STANDARD

1. All user passwords must be changed at least quarterly (every 90 days);
2. Passwords must never be inserted into email messages or other forms of electronic communication;
3. Where SNMP is used, the community strings must be defined as something other than the standard defaults of "public," "private" and "system" and must be different from the passwords used to log in interactively. A keyed hash must be used where available (e.g., SNMPv2);
4. Passwords shall not be shared with, used by, or disclosed to others. Use of Generic or group passwords shall only be used when there is a documented business reason for doing so and must be approved in advanced by the Cyber Security manager;
5. Systems will use an account lockout process when available that locks the account after three failed attempts. Manual action by a system administrator may be required to reactivate account. See lockout policy below;
6. Passwords will not be transmitted across the network in "clear" text;
7. Passwords will be not visible on a screen, hardcopy, or on any other output device;
8. Vendor or service accounts will be removed or renamed and default passwords changed prior to deployment;
9. Administrative account passwords will be changed promptly upon departure of personnel (mandatory or voluntary) or suspected compromise of the password. User accounts will be disabled promptly upon departure of personnel (mandatory or voluntary).

Password Requirements

1. Must not have been used recently (in your last 12 passwords).
2. Must be at least 8 characters in length (longer is strongly encouraged).
3. Cannot contain your USERName.
4. Must contain 3 of the following 4 requirements:
    a. Must have upper case letters (A-Z).
    b. Must have lower case letters (a-z).
    c. Must have at least one number (0-9).
    d. Must have at least one special character (! @ # $ % ^ & * ( ) [ ] { }, etc.).

GENERAL PASSWORD GUIDELINES

1. Effective passwords will have the following characteristics:
    a. Are not a word in any language, slang, dialect, jargon, etc.
    b. Are not based on personal information, names of family, etc.
    c. Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is create a password based on a phrase.

2. Poor, weak passwords may have the following characteristics:
    a. The password is a word found in a dictionary (English or foreign)
    b. The password is a common usage word such as:
        i. Names of family, pets, friends, co-workers, fantasy characters, etc.
        ii. Computer terms and names, commands, sites, companies, hardware, software.
    c. Birthdays and other personal information such as addresses and phone numbers.
    d. Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
    e. Any of the above spelled backwards.
    f. Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

3. Password Protection
    a. Do not use the same password for ITD accounts as for other non-ITD access (e.g., personal ISP accounts, etc.).
    b. Do not share passwords with anyone, including administrative assistants or secretaries.
    c. All passwords are to be treated as sensitive, Confidential information.
    d. Don't reveal a password over the phone to ANYONE
    e. Don't reveal a password in an email message
    f. Don't reveal a password to the boss
    g. Don't talk about a password in front of others
    h. Don't hint at the format of a password (e.g., "my family name")
    i. Don't reveal a password on questionnaires or security forms
    j. Don't share a password with family members
    k. Don't reveal a password to co-workers while on vacation
    l. If someone demands a password, refer them to this document or have them contact the Cyber Security Office
    m. Do not use the "Remember Password" feature of applications or web pages
    n. Do not write passwords down and store them anywhere in your office.
    o. Do not store passwords in a file on ANY computer system (including Palm Pilots or similar devices) without encryption.
    p. If an account or password is suspected to have been compromised, report the incident immediately and change all passwords.

Lock-out Policies

Incorrect attempts at logging in may indicate an attempt to break into a network using an employee's user account. In order to prevent this, the account will be locked after Five (5) consecutive incorrect attempts to log in. Accounts can be unlocked by administrators, or users may wait fifteen minutes for the account to be open again.

All computers shall be configured to have a password-enabled screen saver that is to be configured to activate after a period of user inactivity. The inactivity time period should be set to a reasonable value, with the recommendation being 20 minutes. A shorter time delay is encouraged. This security-lockout feature shall automatically initiate after the desktop computer remains idle from user interaction. The user must then reenter their password to gain access to the computer. All users are encouraged to screen-lock their computers (Windows-L) when they leave their desks for more than a couple minutes.

REFERENCES

ITD Security Policy A-22-09

ITD Computer, Email and Internet Usage Policy A-22-02

ITRMC Guideline G560 - http://www2.state.id.us/itrmc/plan&policies/guidelines/g560.htm