

**Policy Description:**

PASSWORD POLICY

Policy No: ODT – IT – 002

Authorities:

OIT Policy No. ITP B.3

Division With Primary Responsibility:

Information Services

Pages: 4 Pages

Effective Date: July 15, 2005

Revised Date: February 1, 2007

1. Policy Overview

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of the Ohio Department of Taxation's (ODT's) entire network. As such, all ODT employees (including contractors and vendors with access to ODT systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

2. Policy Purpose

The purpose of this policy is to outline general password guidelines, and to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

3. Policy Scope

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any ODT facility, has access to the ODT network, or stores any non-public ODT information.

4.0. Policy

4.1. General

- Passwords must be a minimum of eight characters in length except for PDA's which must be a minimum of four characters.
- Passwords must be a combination of alpha and numeric characters.
- Passwords can not be reused for a period of 18 months.

- All system-level passwords (e.g., root, Windows administrator, application administrator accounts, etc.) must be changed on a regular basis. System level accounts are maintained and managed by the ISD Security Unit.
- All user-level passwords (e.g., desktop computer, mainframe, etc.) must be changed every 90 days.

- User accounts will be locked after a maximum of three unsuccessful attempts to gain access to an ODT computer system. Exceptions: The Windows threshold is set to ten unsuccessful attempts according to Microsoft's recommendation; PDA's are set to five attempts.
- Users are required to complete a System Security Request (SSR) to have an account unlocked and/or a password reset.
- The ISD Security Unit or its delegates are responsible for resetting passwords and/or unlocking user accounts.
- User accounts are associated with a single individual and will not be established for use by more than one person. A very limited number of accounts for generic use have been established for general/public use PC's, Test Lab PC's, and Interview Testing PC's.
- Passwords of employees, contractors, temporary personnel or other agents of the state who have terminated or transferred to other work units will be deactivated. Passwords will be deactivated for such users not later than the end of business on the effective date. A terminated user's passwords will not be retained beyond termination date. Passwords associated with involuntary terminations will be deactivated immediately upon notification.
- Passwords must not be inserted into e-mail messages sent to external email addresses unless the information is being sent using SecureMail Gateway.
- Passwords can be emailed to internal ODT email accounts if they are encrypted.
- All default application and system passwords MUST be reset before deployment of any system or application.
- All user-level and system-level passwords must conform to the guidelines described below.

4.2. Policy Guidelines

A. General Password Construction Guidelines

Passwords are used for various purposes at ODT. Some of the more common uses include: user level accounts, Web accounts, e-mail accounts, screen saver protection, voicemail password, and local router log-ins. Everyone should be aware of how to select strong passwords.

Poor, weak passwords have the following characteristics:

- The password contains less than eight characters
- The password is a word found in a dictionary (English or foreign)
- The password is a common usage word, such as:
 - Names of family, pets, friends, coworkers, fantasy characters, etc.
 - Computer terms and names, commands, sites, companies, hardware, software
 - The words "Ohio Department of Taxation" or any derivation
 - Birthdays and other personal information such as addresses and phone numbers
 - Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
 - Any of the above spelled backwards

- Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

Strong passwords have the following characteristics:

- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters, e.g., 0-9,!@#\$%^&*()_+|~-=\`{ }[]:”;'<>?,./)
- Are at least eight alphanumeric characters long
- Are not words in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.
- Passwords should never be written down or stored online. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: “This May Be One Way To Remember” and the password could be: “TmB1w2R!” or “Tmb1W>r~” or some other variation.

Note: **DO NOT** use any of these examples as passwords!

B. Password Protection Standards

Do not use the same password for ODT accounts as for other non-ODT access (e.g., personal ISP account, option trading, benefits, etc.).

Do not share ODT passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, confidential ODT information.

Here is a list of “don’ts”:

- Don’t reveal a password over the phone to ANYONE.
- Don’t reveal a password in an e-mail message.
- Don’t reveal a password to your supervisor.
- Don’t talk about a password in front of others.
- Don’t hint at the format of a password (e.g., “my family name”).
- Don’t reveal a password on questionnaires or security forms.
- Don’t share a password with family members.
- Don’t reveal a password to coworkers while you are away on vacation.

If someone demands a password, refer them to this document or have them contact someone in the ISD Security Unit. The Security Unit will work with management to resolve the issue.

Do not use the “Remember Password” or “Save Password” feature of applications (e.g., Lotus Notes, Outlook, Internet Explorer, etc.).

Do not write passwords down and store them anywhere in your office or with your laptop. Do not store passwords in a file on ANY computer system (including Palm Pilots or similar devices) without encryption.

Change user level passwords at least every ninety days (system-level passwords may be managed at a different interval).

If an account or password is believed to have been compromised, report the incident to the ISD Security Unit or Customer Response Center and change the password immediately.

The ISD Security Unit or its delegates may perform password cracking or guessing on a periodic or random basis. If a password is guessed or cracked during one of these scans, the user will be required to change it.

C. Application Development Standards

Application developers must ensure their programs contain the following security precautions. Applications must:

- Not store passwords in clear text or in any easily reversible form.
- Provide for role management, so that one user's access can be easily transferred to another user.
- Support TACACS+, RADIUS, and/or X.509 with LDAP security retrieval, unless a wavier is obtained from the ISD Security Unit.

5. Definitions

Terms	Definitions
Application administration account	Any account that is for the administration of an application (e.g., Windows Administrator, root, etc.).

6. Revision History

Effective Date	Description
02/01/2007	4.1 Identified PDA passwords; thresholds for unsuccessful attempts; multiple user PC passwords; exceptions for SecureMail Gateway

7. Declaration

I have read and acknowledge receipt of the Password Policy revised February 1, 2007 number ODT-IT-002.

Employee Printed Name

Badge Number

Employee signature

Date