Massachusetts Department of
Workforce
Development

Password Policy

DOCUMENT REVISION HISTORY

Date	Version	Author	Comments
10/11/06	1.0	Jim Newman	Initial Submission

TABLE OF CONTENTS

1.0 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 DWD's entire network. As such, all users of the DWD network (including employees, partners, contractors and vendors with access to DWD systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

2.0 Purpose

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change. This policy is written using the guidance and best practices outlined in NIST Special Publication 800-14 (National Institute of Standards and Technology) and the recommendations of the Center for Internet Security.

3.0 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 DWD facility, has access to the DWD network, or stores any non-public DWD information.

4.0 Policy

4.1 General

- Users must select their own passwords
- Users will be directed to choose a "strong" password, as defined in the Guidelines below
- Passwords must be at least eight (8) characters in length
    - Passwords must contain characters from at least three of the following four categories:
        - English uppercase characters (A — Z)
        - English lowercase characters (a — z)
        - Base 10 digits (0 — 9)
        - Non-alphanumeric (For example: !, $, #, or %)
    - Users will not be allowed to use the same password as had been used in the four (4) previous occurrences and/or the previous 90 days, whichever is greater
- Passwords must be safeguarded
    - Passwords must not be shared
        - If compromised, report the incident to Internal Control and Security and immediately choose a new password(s)
    - Individuals are responsible for keeping their passwords secure
    - If another co-worker or supervisor demands to learn your password, refer them to this document and report the incident to Internal Control & Security
    - Do not use the "Remember Your Password" feature of applications

- Passwords will expire in 90 days, and must be changed by the user prior to that time.
    - If you believe that your password has been compromised, immediately change your password (procedures will differ among systems). Report the incident to Internal Control and Security
- Initial User passwords will be assigned by an Administrator and communicated to the user.
- When a system is replaced, or a new system is developed, it will meet the requirements of this password policy.
- All system-level passwords (e.g., root, enable, Windows admin, application administration accounts, etc.) must be changed on at least a quarterly basis.
- All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every ninety days.
- User accounts that have system-level privileges granted through group memberships or programs must have a unique password from all other accounts held by that user.
- Passwords must not be inserted into email messages or other forms of electronic communication.
- All user-level and system-level passwords must conform to the guidelines described below.

4.2 Guidelines

A. General Password Construction Guidelines

Passwords are used for various purposes at DWD. Some of the more common uses include: user level accounts, web accounts, email accounts, screen saver protection, and local router logins. Since very few systems have support for one-time tokens (i.e., dynamic passwords which are only used once), everyone should be aware of how to select strong passwords.

Poor, weak passwords have the following characteristics:

- The password contains fewer 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, co-workers, fantasy characters, etc.
    - Computer terms and names, commands, sites, companies, hardware, software.
    - 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 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 on-line. 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 either of these examples as passwords!

B. Password Protection Standards

Do not use the same password for DWD accounts as for other non-DWD access (e.g., personal ISP account, credit cards, bank accounts, etc.). Where possible, don't use the same password for various DWD access needs. For example, select one password for the UI Benefit system and a separate password for the MOSES system. Also, select a separate password to be used for a network account and an application account.

Do not share DWD passwords with anyone, including administrative assistants or Help Desk staff. All passwords are to be treated as sensitive, confidential DWD 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 email message
- Don't reveal a password to your supervisor or manager
- 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 co-workers while on vacation

If someone demands a password, refer them to this document or have them call someone in the Internal Control and Security Unit.

Do not use the "Remember Password" feature of applications (e.g. Internet Explorer).

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

Change passwords at least every 90 days (except system-level passwords which must be changed quarterly).

If an account or password is suspected to have been compromised, report the incident to Internal Control and Security and change all passwords.

Password cracking or guessing may be performed on a periodic or random basis by Internal Control and Security or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it.

C. Application Development Standards
When a system is replaced, or a new system is developed, it will meet the requirements of this password policy.

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

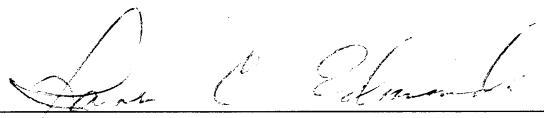
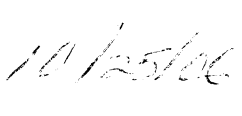
- should support authentication of individual users, not groups.
- should not store passwords in clear text or in any easily reversible form.
- should provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.

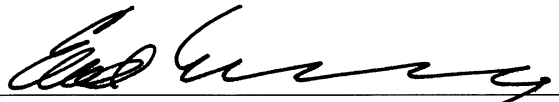
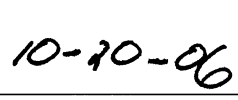
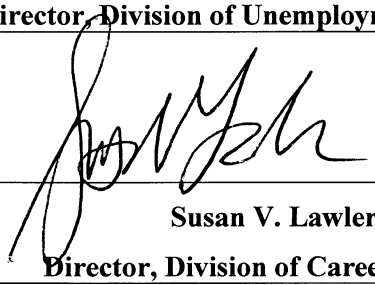
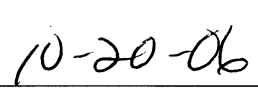
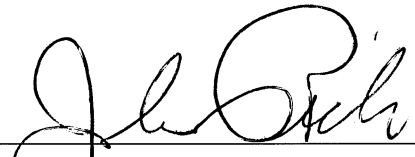
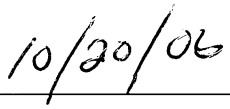
5.0 Enforcement

Any user of the DWD network found to have violated this policy may be subject to disciplinary action. The disciplinary action imposed may vary from denial of access to the DWD network (for non-DWD employees / users) up to and including termination of employment (for DWD employees).

6.0 Governance

Responsibility for adoption and/or implementation of this policy is as follows:

Executive Approval	
	
Jane C. Edmonds **Director, Department of Workforce Development**	**Date**

Divisional Approvals	
	
Ed Malmborg **Director, Division of Unemployment Assistance**	**Date**
	
Susan V. Lawler **Director, Division of Career Services**	**Date**
	
John Rich **Director, Division of Apprentice Training**	**Date**

Approving Body	
Information Technology Security Committee	