

State of Vermont

User Password Policy and Guidelines

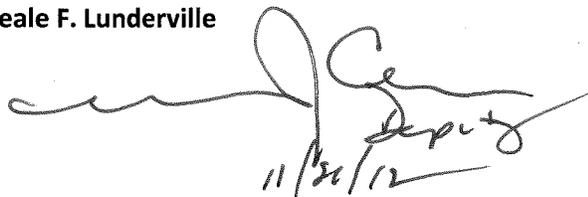


Date of Rewrite Approval: 10/2009

Originally Approved: 4/08/2005

Approved by: Neale F. Lunderville

Policy Number:

A handwritten signature in cursive script, followed by the word "Deputy" and the date "11/20/12".

Contents

1.0 Introduction	3
1.1 Authority	3
1.2 Purpose	3
1.3 Scope	3
2.0 Policy	4
2.1 General	4
2.2 Password Usage	4
2.3 Password Change	4
2.4 Password Reuse	5
3.0 Password Protection	5
Appendix A: General Password Construction and Guidelines	6

1.0 Introduction

1.1 Authority

The State of Vermont is authorized to undertake the development of enterprise architecture policies and standards. The Department of Information and Innovation (DII) is authorized “to provide direction and oversight for all activities directly related to information technology, including telecommunications services, information technology equipment, software, accessibility, and networks in state government.” See 22 VSA §901(1).

Managers, employees, records personnel, third party vendors and all others who connect to or handle State of Vermont networks and data are responsible for reviewing this policy in concert with business, legal, and information technology staff. Each must ensure this policy (1) satisfies each agency’s and/or department’s legal requirements, and (2) that its data requirements can be effectively performed by State employees. If applicable State laws or regulations require more stringent requirements, each agency must adopt its own policy explicitly stating the more stringent legal requirements. Agencies shall not develop an internal policy that lowers the minimum requirements listed in this policy.

1.2 Purpose

Passwords are an important component of information technology and network security. The use of a password in combination with the user name serves to authenticate those who are authorized to have access to system resources and information assets. Authenticated access is one way that the enterprise can be assured that systems and data are being used appropriately. As such, passwords must be constructed, used, changed on a regular basis and protected appropriately to ensure that the level of security they imply is actually met.

The purpose of this policy is to assure that data and systems are protected appropriately by specifying requirements for authenticated access.

1.3 Scope

The scope of this policy applies to all devices that have access to State of Vermont data or networks, except those whose dedicated purpose is to provide the public with access to information.

2.0 Policy

Passwords are the foundation of virtually all access and user management security systems. Passwords typically allow access to the data managed and controlled by departments and agencies. There may be instances where two factor authentication or biometrics may be required to access specific accounts or stricter password configuration requirements are needed. If that is the case, this should be reflected in a specific agency or department written procedure and/or policy.

This policy states the minimum requirements for passwords for the State of Vermont. If agencies or departments require more rigorous passwords, they will be responsible to appropriately document those requirements.

2.1 General

In general, passwords will be strong. A “strong” password is defined as follows:

Be a minimum of eight (8) characters in length, must use at least three of the four character types, those being: lower case letters, upper case letters, numbers and special characters (Example: !, #, %). An example of a strong password is: PrI2Ks!*. This password comes from the phrase: “Passwords are important to keep safe!*” It is a strong password because it has all of the elements required. It is also easy to remember. *Note: DO NOT use this as a password!*

2.2 Password Usage

The use of strong passwords may not be practical in all situations, such as on smartphones, tablets or devices that do not access or store data protected by Federal or State regulation, statute or law. A minimum four digit PIN password or other equitable setting must be enabled.

However, mobile devices as well as desktops and laptops that contain or gain access to data protected by Federal or State regulation, statute or law require a strong password (as defined in section 2.1) to be entered prior to gaining access to such data.

2.3 Password Change

1. All device passwords must be changed twice a year (every 180 days), at minimum, to reduce the risk of compromise through guessing, password cracking or other attack and penetration methods.

Departments or agencies dealing with data that is protected by Federal or State regulation, statute or law, requiring that more stringent password requirements must be followed, will develop appropriate documentation to meet these more stringent requirements.

If a user terminates for any reason, passwords and accounts should be disabled immediately by the appropriate IT department personnel.

2. Password changes shall be systematically enforced where possible.
3. Where possible, passwords shall be systematically disabled after ninety days of inactivity.

2.4 Password Reuse

In general, reusing passwords diminishes the security of the systems they protect. To minimize this risk, passwords may only be reused every third password, at minimum. As such a completely new password is required for the first two expires; thereafter, the first password can be reused. "Completely new" is defined as having at least fifty percent (50%) of the characters different from the previous password.

3.0 Password Protection

For passwords to be effective there are general rules that must be observed. These rules are listed below:

1. Passwords are to be treated as confidential information and shall not be shared with non-authorized individuals.
2. Should a request be made that does not conform to this policy, the employee should immediately inform both the IT department and his/her direct manager, as the person making the request may not actually work for the IT department, but may be a Social Engineer looking for access information.
3. Written records of passwords may be kept in a secure location such as a locked drawer, room or safe. Electronic records may be kept on encrypted devices such as a USB drive. Passwords should never be posted in easily accessible areas such as on monitors or keyboards.
4. If an employee either knows or suspects that his/her password has been compromised, he/she must report it to his/her IT department and department supervisor, and must immediately change the password.

Appendix A: General Password Construction and Guidelines

Passwords are used for various purposes within the State of Vermont agencies and departments as well as by vendors, contractors and other approved persons. Some of the more common uses include: user level accounts, Web accounts, e-mail accounts, screen saver protection and voicemail password. Since very few systems support one-time tokens, (i.e., dynamic passwords that are used only once), everyone should be aware of how to select strong passwords.

Do not use the same password for State of Vermont accounts as for other non-work related account access (e.g., personal Internet accounts, home computer access accounts, social networking accounts, etc.)

Passwords should always be stored in a secure fashion. If you do write down your passwords, keep them in a locked drawer or other secure location. If you store them online, be sure they are encrypted.

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: “Tmb1W>r~” or some other variation. *Note: Do NOT use either of the examples in this policy as passwords!*

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.
- Is not a word in any language, slang, dialect, jargon, etc.
- Passwords should not be based on well-known or easily accessible information, including personal information. They should not be words commonly found within a standard dictionary.
- Are not based on personal information, names of family, pets etc.