Password Protection Policy

ChilledWeb Limited

Policy Name:	Password Protection Policy	Policy Ref:	CWPPAP
Date of Last Revision:	18 February 2023	Version No:	3.6

Contents

PASSWORD PROTECTION POLICY 1

ChilledWeb Limited 1

CONTENTS 1

OVERVIEW 2

PURPOSE 2

SCOPE 2

POLICY 2

Password Creation 2

Password Change 3

Password Protection 3

Application Development 3

Use of Passwords and Passphrases 4

EXCEPTIONS 4

NON-COMPLIANCE 4

Overview

Passwords are an important aspect of computer security. A poorly chosen password may result in unauthorised access and/or exploitation of ChilledWeb's resources. All users, including contractors and vendors with access to ChilledWeb systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

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.

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

Policy

Password Creation

- All user-level and system-level passwords must conform to the ChilledWeb Password Construction Policy.
- Users must not use the same password for ChilledWeb accounts as for other non-ChilledWeb access (for example, personal ISP account, option trading, benefits, and so on).
- Where possible, users must not use the same password for various ChilledWeb access needs.
- User accounts that have system-level privileges granted through group memberships or programs such as sudo must have a unique password from all other accounts held by that user to access system-level privileges.
- Where Simple Network Management Protocol (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. SNMP community strings must meet password construction guidelines.

Password Change

- All system-level passwords (for example, root, enable, admin, application administration accounts, and so on) must be changed every 30 (thirty) days.
- All user-level passwords (for example, email, web, desktop computer, and so on) must be changed every 30 (thirty) days.
- Password cracking or guessing may be performed on a periodic or random basis by the Directors or their delegates. If a password is guessed or cracked during one of these scans, the user will be required to immediately change it to be in compliance with the Password Construction Guidelines.

Password Protection

- Passwords must not be shared with anyone. All passwords are to be treated as sensitive, Confidential ChilledWeb information.
- Passwords must not be inserted into email messages or other forms of electronic communication.
- Passwords must not be revealed over the phone to anyone.
- Do not reveal a password on questionnaires or security forms.
- Do not hint at the format of a password (for example, "my family name”).
- Do not share ChilledWeb passwords with anyone, including administrative assistants, secretaries, managers, co-workers while on vacation, and family members.
- Do not write passwords down and store them anywhere in your office. Do not store passwords in a file on a computer system or mobile devices (phone, tablet) without encryption.
- Do not use the "Remember Password" feature of applications (for example, web browsers).
- Any user suspecting that his/her password may have been compromised must report the incident and change all passwords immediately to their supervisor.

Application Development

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

- Applications must support authentication of individual users, not groups.
- Applications must support the locking of individual user accounts after three unsuccessful logon attempts.
- Applications must not store passwords in clear text or in any easily reversible form.
- Applications must not transmit passwords in clear text over the network.
- Applications must 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.

Use of Passwords and Passphrases

Passphrases are generally used for public/private key authentication. A public/private key system defines a mathematical relationship between the public key that is known by all, and the private key, that is known only to the user. Without the passphrase to "unlock" the private key, the user cannot gain access.

Passphrases are not the same as passwords. A passphrase is a longer version of a password and is, therefore, more secure. A passphrase is typically composed of multiple words. Because of this, a passphrase is more secure against "dictionary attacks."

A good passphrase is relatively long and contains a combination of upper and lowercase letters and numeric and punctuation characters. An example of a good passphrase:

"The*?#>*@TrafficOnTheM1Was*&#!#ThisMorning"

All of the rules above that apply to passwords apply to passphrases.

Exceptions

Any exception to the policy must be approved by the Directors in advance.

Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Any program code or application that is found to violate this policy must be remediated within a 30 day period.