Insert Organization Name or Letter Head

Use Strong Users Authentication Policy

Insert Date

**Disclaimer**

**Instructions:** CyberSecure Canada has developed this template for your use in relation to certification requirements for the Use Strong User Authentication security control area. It provides guidance as to how information can be organized and documented for certification. CyberSecure Canada does not guarantee a successful certification from use of this template. Organizations are not obliged to use this template and may provide the certification requirement(s) in a documented format best suited for them.

# Template Instructions

**Instructions:** The purpose of this template is to help users to meet the certification requirements for the UseStrong User Authentication security control area for CyberSecure Canada.

Instructions are provided in blue font within each section of this template.  Upon completion of the template, delete these instructions.

It is recommended that users review the eLearning module for **Use Strong User Authentication** and the completed example of this policy.]

# Revision History

**Instructions:** It is a best practice for organizations to ensure their policies are reviewed and updated regularly. Document what changes are made, when, and by whom. ]

The Uses Strong Users Authentication Policy has been modified as follows:

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Modification | Modifier |
| [date edited] | [document version] | [Description of changes made] | [name of the editor] |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Definitions

|  |  |
| --- | --- |
| Two-Factor Authentication | Authentication used to confirm the identity of a user by validating a combination of two different factors |
| User Authentication | A process used to confirm the identity of a person attempting to access a system or device |
| User Authorization | A process used to assign permissions to limit access to those who need it |
| Password Manager | A software application that creates, stores, and recalls passwords |

# Scope

**Instructions:** Insert your scope statement or use the example below if appropriate to your organization.

This policy shall apply to the use of two-factor authentication and passwords at [Organization Name]. It applies to all employees, contractors, and affiliates of [Organization Name], and shall govern acceptable password use on all systems that connect to the organization’s networks or accesses and/or stores its data.

# Two-Factor Authentication

**Instructions:** Insert your two-factor policy statement(s) and include applicable IT systems. If appropriate, you can use the provided example.

*Two-factor authentication will be used for following system:*

* *Financial accounts*
* *System administrators*
* *Cloud administrators*
* *Privileged users*
* *Senior executives*
* *All remote access*

# Password Creation

**Instructions:** Determine the required length and construction of a password. Longer passwords, or passphrases, are encouraged.

Insert your password creation statement(s). Alternatively, you can use the provided example.

1. *All passwords must be at least* [x] *characters long*
2. *Default passwords must be changed when software and devices are installed*
3. *Administrator and other high value accounts must be* [X or greater] *characters long*
4. The same passwords are not to be used for multiple accounts (for example, work email and server login)

# Password Management

**Instructions:** Decide whether or not to use Password Management software and create a policy on its use.

Determine if and when passwords can be physically written down and stored.

Insert your password management and creation policy statement(s), alternatively you can use the provided example.

1. *Passwords must not be shared with anyone, whether in person or sent electronically*
2. *Auto login for work related services must be disabled*
3. *All passwords must be updated to the standards outlined in the Password Creation section. This also applies to passwords on devices*
4. [Insert selected password manager] *is used to store and manage passwords*
5. *Passwords that are physically written down must be stored securely where no other person can access them*
6. *The organization’s backup plan will include* the backup and recovery of passwords managed by password managers

# Password Updates

**Instructions:** For CyberSecure Canada certification, passwords may remain constant for an indefinite amount of time unless there is suspicion or evidence of compromise. Examples of a compromise include:

• A policy in the password protection category has been breached

• A cyber incident has occurred in which the user account information was compromised

• Any other suspicion of the password being compromised

Your organization can opt to require frequent password updates.

Insert your password update policy statement(s), alternatively you can use the provided example.

1. *Passwords are updated on suspicion or evidence of compromise*
2. *Users are able to update their passwords whenever they choose*

# Enforcement

**Instructions:** Insert your enforcement statements below or use the provided example.

*It is the responsibility of the* [Name or Team] *and to implement the outlined polices. Users are responsible for setting and managing their personal passwords and to use two-factor authentication as outlined above.*

# References

<https://blog.focal-point.com/a-free-password-policy-template-for-2018>

<http://www.itmanagerdaily.com/password-policy-template/>

# Additional Certification Requirements

# Usage of Two-Factor Authentication

|  |
| --- |
| **Instructions:** Provide an overview of how your organization uses two-factor authentication. |

# Exceptions to Usage of Two-Factor Authentication

|  |
| --- |
| **Instructions:** Identify devices that will not adhere to two-factor authentication and the rationale for exemption. |