Password policy (BASIC)

 Template

# Authority and review

## Document control and review

|  |  |
| --- | --- |
| **Document check**  |  |
| Author  |  |
| Owner |  |
| Date created |  |
| Last revised by  |  |
| Last revision date |  |

.

## Version management

|  |  |  |  |
| --- | --- | --- | --- |
| **Version**  | **Date of approval** | **Approved by**  | **Description of change** |
| 1.0 |  |  |  |

# Intro

Passwords are often used to authenticate users. This document provides a policy for the use and implementation of passwords for confidential and critical information systems.

We used to think that the best way to secure passwords was to make them strong and change them often. Nowadays, the new philosophy of making passwords long but user-friendly is gaining popularity. Multi-factor authentication is strongly encouraged and should be used whenever possible, not only for work-related accounts but also for personal accounts.

This policy document is part of a set of policy documents that support **[Organisation]** in establishing a sound strategy around cybersecurity.

# Password settings

## Password strength

Password strength is important to reduce the chances of misuse.

Password systems should enforce the use of strong passwords according to these rules:

* The minimum permitted length of the password must be adhered to **(minimum X characters, X is recommended)**
* Administrator passwords must contain a minimum of **XX** characters
* Passwords for service accounts must be at least **XX** characters long
* Very long passwords should be allowed (e.g. 256 characters)
* Passwords containing your username should be rejected
* Passwords containing your first or last name should be rejected
* Complex passwords must be enforced, containing at least three of the following categories:
	+ - Uppercase letters (A-Z)
		- Lowercase letters (a-z)
		- Digits (0-9)
		- Special characters: !@#$%^&\*() etc

Exceptions:

In the following cases, a password of at least 4 digits is allowed:

* If the code is an addition of a physical access ID such as a smart card or token
* If the system is not connected to a network and has strong physical security controls
* To unlock the screen of an **[Organisation]** mobile device such as a smartphone or tablet

## Password change policy

To reduce the risk of compromising passwords, they should be changed regularly. The following rules apply:

* Default passwords for new devices should be changed.
* Systems should allow users to change passwords at any time.
* Periodic password changes should be enforced depending on the system's enforced minimum password length
* When the system's minimum allowed password length is **X** characters, users should be forced to change passwords every **X** months (or **XX** days).
* When the system's minimum allowed password length is **XX** characters, users should be forced to change passwords every **X** months (or **XX** days).
* Passwords provided by others than the user himself (e.g. the ICT department) should be changed at the first login.
* Password systems should explicitly deny reuse of at least the last **X** passwords.
* Shared passwords known to people leaving the organisation should be changed.

Exceptions:

The policy of changing passwords is recommended but not mandatory in the following cases:

* If the password is used for a service account and cannot be used for interactive login
* If the code is an addition of a physical access ID such as a smart card or token
* If the system is not connected to a network and has strong physical security controls
* To unlock the screen of an **[Organisation]** mobile device such as a smartphone or tablet

## Prevention of attacks

Systems should have at least one mechanism to prevent brute force attacks. Examples of such techniques are:

* **Account lockout:**
An exclusion policy disables login functionality for a specific account. (e.g. Lock account for **XX** minutes after **X** failed login accounts).
* **Black IP list**:
Like account blocking policies, this mechanism detects failed login attempts, but it checks which IP addresses the login request comes from. If too many attempts are detected (e.g. 20) from a particular IP address, that address is blacklisted.
* **Login delay:**This mechanism adds an incremental repeat delay after a wrong password is used. (e.g. wait 0.5 seconds after 2 failed attempts, 1 second after the third failure, 2 seconds after the fourth, 4 seconds after the fifth, etc.).

# Password protection

* Passwords should not be shared with anyone, including supervisors and colleagues. All passwords should be treated as sensitive, confidential information of **[Organisation**]
* Passwords should not be included in e-mail messages or other forms of electronic communication, or communicated to anyone by phone.
* Passwords should only be stored in password managers authorised by the organisation. Passwords on paper should be avoided unless there is strong physical security (such as a safe).
* Do not use the "Remember password" feature of applications (e.g. web browsers).
* Anyone who suspects their password has been compromised should report it and change all relevant passwords.

## Distribution via e-mail

Distributing usernames and passwords via e-mail can be efficient and convenient. Although e-mail is not the most secure medium by default, it can be used when:

* No external e-mail system is used.
* Email is sent encrypted (like Office 365)
* The specified combination of username and password expires after the first use or, if not used, after **1 month.**

## Distribution via SMS

SMS is not a secure protocol and should never be used to send username and password combinations. It can be used to send partial login information, but only if the following conditions are met:

* The message contains at most only one part of the combination: system, username, password or token. The other parts are sent via other distribution methods.
* The user expects the message and is therefore likely to use it soon.
* The information in the message expires after the first use or, if not used, after 1 month.