ACCESS 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

Within **[organisation]** , access management is an essential component of security that determines who has access to certain data, applications and other digital assets, and under what circumstances. These access management policies secure digital environments in the same way that keys and guest lists secure physical spaces. In other words, they let the right people in and keep other people out. These policies are built on techniques such as authentication and authorisation. These allow **[organisation]** to verify that users are who they say they are, and that these users have been granted appropriate access, based on context such as device, location, function and more.

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

# Access management

**[organisation]** applies the principle of minimum access. This means that every internal or external user within **[organisation]** is given exactly sufficient access(s) to the information and systems they need to perform their function properly. Moreover, **[organisation]** prefers to implement and enforce standard Multifactor Authentication (MFA) where possible

Remote access to **[organisation]'**s critical and confidential systems from an untrusted location, such as the employee's home or client's office, should be restricted to designated users. **[organisation's]** laptops are equipped with settings to establish a VPN connection to **[organisation's]** systems.

Granted accesses shall be checked at regular intervals and modified if necessary. Adjustments relating to access, including remote work, are communicated in a timely manner to the **[person responsible within the organisation]** by means of an Account Creation/Modificaton Form (ACMF) or an Account Removal Form (ARF) (**see ANNEX 1 Forms**)

# Account management

## User accounts

User accounts are a common way of providing authentication. The following rules apply to user accounts for accessing critical and confidential systems:

* should be unique and personal.
* must be password protected, as described in the Password Policy.
* new user accounts for employees can only be requested by an authorised person and processed.
* should be withdrawn when they become obsolete (e.g. upon termination of the contract).

## Privileged accounts

The assignment of accounts with privileges (e.g. domain administrator, super user and root) should be restricted. Privileged accounts should be used only when privileged access is needed. Owners of such accounts should use a non-privileged account for normal user activities. For example, system administrators should not use their Domain Administrator account to handle their e-mail.

The name of this account should not disclose information about the account's extended privileges, this is to prevent abuse.

For privileged accounts for critical and confidential systems accessed from untrusted networks such as the internet, multifactor authentication should be used

## Shared accounts

The use of shared accounts should be prevented. If it cannot reasonably be prevented, the use of shared accounts should be controlled. Controls should be in place for:

* Knowing who can use the account.
* Controlling the use of the account.
* Process of password change and communication of the new password.
* Preventing abuse, e.g. upon termination of the contract.

## Accounts for external staff and external companies

The following additional checks should be carried out for accounts for external staff:

* Accounts should be easily identifiable as being for external staff, for example by adding a prefix to the account name or by mentioning it in a description.

Accounts must be revoked at the end of the contract. If this process cannot be fully ensured, the account should automatically expire every **[3 months] unless** renewal is officially approved.

## Service accounts for communication between systems

The following additional checks must be present for service accounts and machine-to-machine communication accounts:

* Accounts should be easily identified as a service account, for example by adding a prefix to the account name or by mentioning it in a description.
* Again, the principle of minimum access applies.
* Interactive use of service accounts should be avoided.

# Authentication and authorisation

**Microsoft Active Directory (AD)** is a centralised authentication and authorisation solution, which allows rights and security settings to be managed across a network. AD is integrated with the Windows environment and allows for delegated management of **[organisation's]** Windows environment.

## Authentication

* Through a secure connection procedure, one should be able to control access to systems and applications.
* The **[IT manager]** must record and monitor every connection attempt, whether successful or not.
* The initial passwords should be securely and directly transmitted to the user.
* These passwords are set to be changed immediately.
* Multifactor authentication should be used where appropriate and feasible.
* The user account should be suspended for a predetermined period if the user makes a predetermined number of failed authentication attempts **[3 attempts]** within a predetermined period **[5 minutes].**
* Access to the system should be suspended when the account has not been used for a predetermined period **[e.g. 90 days]**.

## Authorisation

* Granting or denying accesses to the information systems can only be requested in a timely manner via an Account Creation and Modification Form (ACMF) and/or Account Removal Form (ARF). (see ANNEX 1 Forms)
* This access can only be requested by the HR responsible or the N+1 of the person concerned.
* Before access is granted, **[organisation responsible]** must formally approve. The **[IT responsible]** must grant, update and remove access rights.
* Authorisation groups are used as much as possible and access is granted on a role-based basis.