**Access Control**

|  |  |
| --- | --- |
| Classification: Company Internal Owner: branko@secfix.com [💡 Secfix AI: You indicated that branko@secfix.com is the owner of this access control poli...] | **Document ID**: POL-11 |

# Version and Approval History

Version and Approval History is maintained in Secfix Platform/Policy section - <https://app.secfix.com/policies>

# Table of Contents

[**Version and Approval History 1**](#_heading=h.gjdgxs)

[**Table of Contents 1**](#_heading=h.nb5oue1docli)

[**Scope 2**](#_heading=h.30j0zll)

[**Policy 2**](#_heading=h.tyjcwt)

[**Business Requirements of Access Control 2**](#_heading=h.3dy6vkm)

[Access Control Policy 2](#_heading=h.8sn3eyat1m65)

[Access to Networks and Network Services 2](#_heading=h.1mx48o1b3kyt)

[**User Access Management 3**](#_heading=h.1t3h5sf)

[User Registration and Deregistration 3](#_heading=h.sbk9vykvi9op)

[User Access Provisioning 3](#_heading=h.p1brlo5h6tpr)

[Management of Privileged Access 3](#_heading=h.581hpb4l0x5m)

[User Access Reviews 3](#_heading=h.68cwb3pjzd1n)

[Removal & Adjustment of Access Rights 4](#_heading=h.e7nwihdu8lq8)

[Access Provisioning, Deprovisioning, and Change Procedure 4](#_heading=h.vmm2rvmencjy)

[**User Responsibility for the Management of Secret Authentication Information 4**](#_heading=h.4d34og8)

[**Password Policy 4**](#_heading=h.2s8eyo1)

[**System and Application Access 4**](#_heading=h.17dp8vu)

[Information Access Restriction 4](#_heading=h.6k1ixelyqqdn)

[Secure Log-on Procedures 5](#_heading=h.ea0icmipn1qv)

[Password Management System 5](#_heading=h.9mp5cp6ajyo5)

[Use of Privileged Utility Programs 5](#_heading=h.lvfij867d7ec)

[Access to Program Source Code 5](#_heading=h.kmx9j8qtbuse)

[**Exceptions 5**](#_heading=h.3rdcrjn)

[**Violations & Enforcement 6**](#_heading=h.26in1rg)

[**Appendix A - Access Management Procedure 7**](#_heading=h.sdlc5q5haj8r)

# Scope

This policy is applicable to all Company information systems involved in the processing, storage, or transmission of confidential data, as defined in the POL-14 Data Management Policy. It is mandatory for all Company employees and external parties who have access to Company engineering networks and system resources to adhere to this Policy. For the purposes of this document, Secfix GmbH [💡 Secfix AI: Replaced] will be referred to as "Company" in all subsequent mentions. This terminology is utilized for simplicity and ease of reading. Please interpret all mentions of "Company" as direct references to Secfix GmbH [💡 Secfix AI: Replaced].

# Policy

Access to information computing resources will only be provided to individuals who have a legitimate business need for such access. The granting and removal of access rights will be carried out in accordance with the provisions outlined in this Access Control Policy.

# Business Requirements of Access Control

## Access Control Policy

The Company will adhere to the principle of least privilege when determining the type and level of access provided to individual users. This means that users will only receive the access necessary to carry out their job functions, as determined by the Company's business and security requirements. Any permissions or access rights not explicitly granted will be automatically denied.

To establish and maintain consistent access controls and access rights, the Company will primarily use Role-Based Access Control (RBAC). Whenever possible, permissions and restrictions will be assigned to groups, and individual user accounts may be granted additional permissions with approval from the system owner or an authorized party. For privileged access to production systems, Multi-Factor Authentication (MFA) will be required to enhance security.

## Access to Networks and Network Services

Access to the Company’s networks and network services will be governed by the following security standards:

* **Governance of access to our network and its services adheres to specific security protocols:** Formal documentation is required for technical access to our networks, detailing the standard role involved, the person authorizing access, the person granting it, and the date of authorization.
* **Access to operational networks is reserved for:** Only employees of the Company and external parties bound by a formal agreement, who demonstrate a clear business necessity, are permitted access to operational networks.
* [💡 Secfix AI: You indicated that you do not have an office, so this section about guest net...]
* **Secure Remote Connectivity:** Any remote connection to our operational systems and networks must employ encryption to ensure security.

# User Access Management

The Company mandates that all personnel have a distinct user identifier for system access, and user credentials and passwords should not be shared among different individuals. Users with various levels of access, such as administrators, should be provided with distinct accounts for regular system use and administrative tasks, whenever possible. Root, service, and administrator accounts may utilize a password management system to share passwords for business continuity purposes only. Administrators should only resort to shared administrative accounts when necessary.

## User Registration and Deregistration

Only authorized administrators are allowed to generate new user IDs, and this should only be done after receiving a documented request from authorized individuals. User provisioning requests must include approval from data owners or Company management authorized to grant system access. Before creating an account, administrators should ensure that the account complies with all the Company’s security and system access control policies, including segregation of duties, fraud prevention measures, and access rights restrictions.

User IDs should be promptly deactivated or deleted when users depart from the organization or when their contract work concludes. User IDs must not be reused.

## User Access Provisioning

* New employees and contractors must not be given access to any Company production systems until they have completed all HR onboarding requirements, which may include signing an employment agreement, an intellectual property agreement, and the information security policy.
* Access should be limited to what is essential for performing job duties, and no access should be granted before the official employee start date.
* Access requests and changes in access rights must be documented in an access request ticket or email.
* No permissions should be granted without approval from the system or data owner or management.
* Records of all permission and privilege changes must be retained for a minimum of one year.

## Management of Privileged Access

The granting of administrative rights must be tightly regulated and necessitates approval from the asset owner.

## User Access Reviews

Administrators will conduct access rights reviews for user, administrator, and service accounts on a quarterly basis to ensure that user access is restricted to the systems necessary for their job responsibilities. These access reviews will be documented.

Access reviews may encompass group memberships and assessments of specific or exception-based permissions. Additionally, access rights will be reviewed when there are any job role changes, such as promotions, demotions, or transfers within the organization.

## Removal & Adjustment of Access Rights

Access rights for all users will be promptly revoked upon termination of their employment or contract, or when their rights are no longer required due to a change in job responsibilities or role. The maximum time frame for access termination is set at <24 business hours>.

## Access Provisioning, Deprovisioning, and Change Procedure

You can find the Access Management Procedure for the Company’s systems in Appendix A Access Management Procedure.

# User Responsibility for the Management of Secret Authentication Information

Every Company employee and third-party user is responsible for controlling and managing their individual user passwords. All users must protect their secret authentication information by the Information Security Policy.

# Password Policy

Where feasible, passwords for confidential systems shall be configured according to the Company password policy defined in POL-04 Information Security & Acceptable Use Policy.

# System and Application Access

## Information Access Restriction

Applications must enforce restrictions on access to program functions and information, ensuring that only authorized users and support personnel can access them. These restrictions should align with the defined access control policy and be tailored to meet the specific requirements of each application, as determined by the data owner. The application-specific access control policy should adhere to the Company’s policies regarding access controls and data management. Before implementing an application, it's essential to evaluate the software using specific criteria to determine the access controls and data policies required. These assessment criteria encompass various aspects and considerations, including but not limited to:

* **Information Sensitivity and Classification:** The risk of organizational harm due to the unauthorized disclosure or acquisition of sensitive information.
* **User Access Control Measures:** The accuracy and scope of procedures in place to regulate user permissions for accessing the application and its data.
* **Data Output Restrictions:** Constraints on data outputs, including filtering sensitive information, controlling output processes, and restricting data access to authorized personnel.
* **Access Privilege Management:** Control over the access rights between the application being evaluated and other systems and applications.
* **Application Feature Access Restrictions:** Strategic restrictions on user access to certain features and high-level commands within the application.
* **Monitoring and Audit Trails:** The capability for logging and auditing system activities and data usage.
* **Data Retention and Purging Policies:** Mechanisms for maintaining data integrity and managing the disposal of outdated information.

Every non-essential default account should be eliminated or deactivated before connecting a system to the network. In particular, all default vendor passwords and credentials on the Company’s systems, devices, and infrastructure must be altered before deployment. This requirement covers ALL default passwords, encompassing those for operating systems, security service software, application and system accounts, and where practical, Simple Network Management Protocol (SNMP) community strings.

## Secure Log-on Procedures

Log-on safeguards must be crafted and implemented based on the data's sensitivity and the risk of unauthorized entry, considering the overall security and access control framework.

## Password Management System

Password management systems, specifically 1Password, should be user-friendly [💡 Secfix AI: You indicated you use 1Password for password management, so we've updated the...], aiding the Company’s staff in adhering to password standards through the enforcement of password strength requirements such as minimum length and complexity, where possible.

All password storage and transmission must be secured using suitable cryptographic measures, via hashing or encryption.

## Use of Privileged Utility Programs

Access to utility programs, system files, or other software with the potential to bypass system and application controls or modify system settings should be limited to the fewest necessary staff. Systems must keep records of all instances of system utility use or changes to system configurations. Unnecessary system utilities or other privileged software should be eliminated or deactivated during the system setup and configuration phase.

Prior approval from management is needed before installing or utilizing any ad hoc or third-party system utilities.

## Access to Program Source Code

Entry to program source code and related materials, such as designs, specifications, verification and validation plans, must be rigorously regulated to block the insertion of unauthorized features into software, prevent accidental modifications, and safeguard the Company’s intellectual property.

All access to source code should be justified by business necessity and consistently recorded for subsequent examination and auditing.

# Exceptions

Petitions for a deviation from this Policy should be directed to the CISO [💡 Secfix AI: You indicated that the CISO is responsible for approving exceptions to this p...] for authorization.

# Violations & Enforcement

Any known violations of this policy should be reported to the CISO [💡 Secfix AI: You indicated that the CISO is responsible for handling policy violations, so...]. Violations of this policy can result in immediate withdrawal or suspension of system and network privileges and/or disciplinary action by company procedures up to and including termination of employment.

# 

# Appendix A - Access Management Procedure

At the completion of the onboarding process, HR will send an email that will generate a series of service tickets for access. IT will provision access for all company-wide systems as well as engineering systems for the Members of Technical Staff (MTS) group. Additional access, beyond standard pre-approved access, must be requested and approved by a manager or system owner.

# Access Request/Access Revocation

This process shall be used for requesting new access to the Company Information Systems or requesting access revocation where no longer required. Every access must be previously approved by the requestors supervisor. All requests will be submitted through Clickup ticketing system [💡 Secfix AI: You indicated that you use Clickup for ticket management and prefer using a t...]

## For new employees (part of Onboarding process)

Supervisor to send access request before the start date noting the following:

* Employee full name and role
* Employee status (full-time, freelancers, contractor, working student)
* Employee start date
* List of systems to be accessed
* Level of privileges if above basic with reasoning behind it

## For employees leaving the company (part of Offboarding process)

Supervisor to send the following:

* Employee full name and role
* Date of last working day
* List of all systems accessed by employee
* List of all company equipment used by employee (company laptop, company phone, documents, other hardware)

Based on the information above, the Information Security Management Leader will fill out the form below and coordinate with the Supervisor on completing all offboarding tasks:

|  |
| --- |
| Company Confidential Employee offboarding plan templatePurpose This form defines and regulates the actions for an employee who has left the organization, for whatever reasons. The actions have to be performed latest on the last working day of the employee. Goal The goal of this form is to document the timely revocation of access rights to company information systems and return of company owned equipment used by the employee during employment. Roles Employee supervisor is responsible for making sure each step in this form is completed. System owners are responsible for revoking access to owned systems. Archive Upon completion, this form shall be securely stored in the Company documentation system for record keeping purposes. Offboarding plan for employee <FirstName LastName>  Department: <Department Name>  Location: <City> <office /Home office>  End date of work: <31.01.2024> Additional requests Any access requests or revocation requests that arise during regular business are to be sent by the user with a supervisor in CC.  Please note that this process is applicable for employees, freelancers, working students, contractors and any other personnel doing business with the Company by accessing the Company Information Systems or using the Company’s equipment.  Issued by (Supervisor): <Max Mustermann>  Issue Date: <31.01.2024>  Signature:  <insert digital signature image> \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

# 

# Managing records kept on the basis of this document

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Record name | Storage location | Person responsible for storage | Controls for record protection | Retention time |
| [Authorizations for software installation] – electronic form | Jira | Information Security Management Leader | Records cannot be edited; only Information Security Management Leader has the right to store such records | Records are stored for a period of 3 years |
| [Authorization for access to digital assets, tools, platforms and software] | Jira | Information Security Management Leader | Records cannot be edited; only Information Security Management Leader has the right to store such records | Records are stored for a period of 3 years |
| [Authorization for revocation or change of access to digital assets, tools, platforms and software] | Jira | Information Security Management Leader | Records cannot be edited; only Information Security Management Leader has the right to store such records | Records are stored for a period of 3 years |
| [Authorization for taking assets off-site] – electronic form | Jira | Information Security Management Leader | Records cannot be edited; only Information Security Management Leader has the right to store such records | Records are stored for a period of 3 years |
| [Decision on how each data type may be exchanged] – electronic form | Jira | Information Security Management Leader | Records cannot be edited; only Information Security Management Leader has the right to store such records | Records are stored for a period of 3 years |
| [Incident Report] | Jira | Information Security Management Leader | Records cannot be edited; only Information Security Management Leader has the right to store such records | Records are stored for a period of 3 years |
| [Visitors Log] | Cloud storage | Information Security Management Leader | Records cannot be deleted; only Information Security Management Leader has the right to store such records | Records are stored for a period of 3 years |

Only the Information Security Management Leader or delegate can grant other employees access to any of the above mentioned documents.