# Access Control Policy

**Policy Owner:** Dotan Simha

**Effective Date:** Aug 14, 2024

## Purpose

To limit access to information and information processing systems, networks, and facilities to authorized parties in accordance with business objectives.

## Scope

All Software Products Guilda Ltd. information systems that process, store, or transmit confidential data as defined in the Software Products Guilda Ltd. Data Management Policy. This policy applies to all employees of Software Products Guilda Ltd. and to all external parties with access to Software Products Guilda Ltd. networks and system resources.

## General requirements

Access to information computing resources is limited to personnel with a business requirement for such access. Access rights shall be granted or revoked in accordance with this Access Control Policy.

## Business requirements of Access Control Policy

Software Products Guilda Ltd. shall determine the type and level of access granted to individual users based on the "principle of least privilege." This principle states that users are only granted the level of access absolutely required to perform their job functions, and is dictated by Software Products Guilda Ltd.'s business and security requirements. Permissions and access rights not expressly granted shall be, by default, prohibited.

Software Products Guilda Ltd.'s primary method of assigning and maintaining consistent access controls and access rights shall be through the implementation of Role-Based Access Control (RBAC). Wherever feasible, rights and restrictions shall be allocated to groups. Individual user accounts may be granted additional permissions as needed with approval from the system owner or authorized party.

All privileged access to production infrastructure shall use Multi-Factor Authentication (MFA).

## Access to networks and network services

The following security standards shall govern access to Software Products Guilda Ltd. networks and network services:

- Technical access to Software Products Guilda Ltd. networks must be formally documented including the standard role or approver, grantor, and date
- Only authorized Software Products Guilda Ltd. employees and third-parties working off a signed contract or statement of work, with a business need, shall be granted access to the Software Products Guilda Ltd. production networks and resources
- Software Products Guilda Ltd. guests may be granted access to guest networks after registering with office staff without a documented request
- Remote connections to production systems and networks must be encrypted

## Customer access management

When configuring cross-account access using AWS IAM roles, you must use a value you generate for the external ID, instead of one provided by the customer, to ensure the integrity of the cross account role configuration. A partner-generated external ID ensures that malicious parties cannot impersonate a customer's configuration and enforces uniqueness and format consistency across all customers.

The external IDs used must be unique across all customers. Re-using external IDs for different customers does not solve the confused deputy problem and runs the risk of customer A being able to view data of customer B by using the role ARN of customer B along with the external ID of customer B.

Customers must not be able to set or influence external IDs. When the external ID is editable, it is possible for one customer to impersonate the configuration of another.

## User access management

Software Products Guilda Ltd. requires that all personnel have a unique user identifier for system access, and that user credentials and passwords are not shared between multiple personnel. Users with multiple levels of access (e.g. administrators) should be given separate accounts for normal system use and for administrative functions wherever feasible. Root, service, and administrator accounts may use a password management system to share passwords for business continuity purposes only. Administrators shall only use shared administrative accounts as needed. If a password is compromised or suspected of compromise the incident should be escalated to the information security team immediately and the password must be changed.

## User registration and deregistration

Only authorized administrators shall be permitted to create new user IDs, and may only do so upon receipt of a documented request from authorized parties. User provisioning requests must include approval from data owners or Software Products Guilda Ltd. management authorized to grant system access. Prior to account creation, administrators should verify that the account does not violate any Software Products Guilda Ltd. security or system access control policies such as segregation of duties, fraud prevention measures, or access rights restrictions.

User IDs shall be promptly disabled or removed when users leave the organization or contract work ends in accordance with SLAs. User IDs shall not be re-used.

## User access provisioning

- New employees and/or contractors are not to be granted access to any Software Products Guilda Ltd. production systems until after they have completed all HR on-boarding tasks, which may include but is not limited to signed employment agreement, intellectual property agreement, and acknowledgement of Software Products Guilda Ltd.'s information security policy
- Access should be restricted to only what is necessary to perform job duties
- No access may be granted earlier than official employee start date
- Access requests and rights modifications shall be documented in an access request ticket or email. No permissions shall be granted without approval from the system or data owner or management
- Records of all permission and privilege changes shall be maintained for no less than one year

## Management of privileged access

Software Products Guilda Ltd. shall ensure that the allocation and use of privileged access rights are restricted and managed judiciously. The objective is to ensure that only authorized users, software components, and services are granted privileged access rights. Software Products Guilda Ltd. will ensure that access and privileges conform to the following standard:

- Identify and Validate Users: Identify users who require privileged access for each system and process.
- Allocate Privileged Rights: Provision access rights basing allocations on specific needs and competencies, and adhering strictly to the access control policy.
- Maintain Authorization Protocols: maintain records of all privileged access allocations.
- Enforce Strong Authentication: Require MFA for all privileged access.
- Prevent Generic Admin ID Usage: prevent the usage of generic administrative user IDs
- Ensure Logging and Auditing: Log all privileged logins and activity

## User access reviews

Administrators shall perform access rights reviews of user, administrator, and service accounts on a quarterly basis to verify that user access is limited to systems that are required for their job function. Access reviews shall be documented.

Access reviews may include group membership as well as evaluations of any specific or exception-based permission. Access rights shall also be reviewed as part of any job role change, including promotion, demotion, or transfer within the company.

## Removal & adjustment of access rights

The access rights of all users shall be promptly removed upon termination of their employment or contract, or when rights are no longer needed due to a change in job function or role. The maximum allowable time period for access termination is 24 business hours.

## Access provisioning, deprovisioning, and change procedure

The Access Management Procedure for Software Products Guilda Ltd. systems can be found in Appendix A to this policy.

## Segregation of duties

Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of Software Products Guilda Ltd. assets. When provisioning access, care should be taken that no single person can access, modify or use assets without authorization or detection. The initiation of an event should be separated from its authorization. The possibility of collusion should be considered when determining access levels for individuals and groups.

## User responsibility for the management of secret authentication information

Control and management of individual user passwords is the responsibility of all Software Products Guilda Ltd. personnel and third-party users. Users shall protect secret authentication information in accordance with the Information Security Policy.

## Password policy

- Where feasible, passwords for confidential systems shall be configured to have at least eight (8) or more characters, one upper case, one number
- Systems shall be configured to remember and prohibit reuse of passwords for last 16 passwords used
- Passwords shall be set to lock out after 6 failed attempts
- Passwords shall expire after 90 days
- For manual password resets, a user's identity must be verified prior to changing passwords
- Do not limit the permitted characters that can be used
- Do not use secret questions (place of birth, etc.) as a sole password reset requirement
- Require the current password in addition to the new password during password change
- Verify newly created passwords against common passwords or leaked passwords databases
- Check existing user passwords for compromise regularly
- Store passwords in a hashed and salted format using memory-hard or CPU-hard one-way hash function
- Enforce appropriate account lockout and brute force protection on account access

## Information access restriction

Applications must restrict access to program functions and information to authorized users and support personnel in accordance with the defined access control policy. The level and type of restrictions applied by each application should be based on the individual application requirements, as identified by the data owner. The application-specific access control policy must also conform to Software Products Guilda Ltd. policies regarding access controls and data management.

Prior to implementation, evaluation criteria are to be applied to application software to determine the necessary access controls and data policies. Assessment criteria include, but are not limited to:

- Sensitivity and classification of data.
- Risk to the organization of unauthorized access or disclosure of data
- The ability to, and granularity of, control(s) on user access rights to the application and data stored within the application
- Restrictions on data outputs, including filtering sensitive information, controlling output, and restricting information access to authorized personnel
- Controls over access rights between the evaluated application and other applications and systems
- Programmatic restrictions on user access to application functions and privileged instructions
- Logging and auditing functionality for system functions and information access
- Data retention and aging features

All unnecessary default accounts must be removed or disabled before making a system available on the network. Specifically, vendor default passwords and credentials must be changed on all Software Products Guilda Ltd. systems, devices, and infrastructure prior to deployment. This applies to ALL default passwords, including but not limited to those used by operating systems, software that provides security services, application and system accounts, and Simple Network Management Protocol (SNMP) community strings where feasible.

## Secure log-on procedures

Secure log-on controls shall be designed and selected in accordance with the sensitivity of data and the risk of unauthorized access based on the totality of the security and access control architecture.

## Password management system

Systems for managing passwords should be interactive and assist Software Products Guilda Ltd. personnel in maintaining password standards by enforcing password strength criteria including minimum length, and password complexity where feasible.

All storage and transmission of passwords is to be protected using appropriate cryptographic protections, either through hashing or encryption.

## Use of privileged utility programs

Use of utility programs, system files, or other software that might be capable of overriding system and application controls or altering system configurations must be restricted to the minimum personnel required. Systems are to maintain logs of all use of system utilities or alteration of system configurations. Extraneous system utilities or other privileged programs are to be removed or disabled as part of the system build and configuration process.

Management approval is required prior to the installation or use of any ad hoc or third-party system utilities.

## Access to program source code

Access to program source code and associated items, including designs, specifications, verification plans, and validation plans shall be strictly controlled in order to prevent the introduction of unauthorized functionality into software, avoid unintentional changes, and protect Software Products Guilda Ltd. intellectual property.

All access to source code shall be based on business need and must be logged for review and audit.

## Exceptions

Requests for an exception to this Policy must be submitted to the CTO for approval.

## Violations & enforcement

Any known violations of this policy should be reported to the CTO. Violations of this policy can result in immediate withdrawal or suspension of system and network privileges and/or disciplinary action in accordance with company procedures up to and including termination of employment.

## Version history

| Version | Date | Description | Author | Approver |
|---|---|---|---|---|
| 2.0 | Aug 14, 2024 | Version 2.0 | Dotan Simha | Dotan Simha |
| 1.0 | Aug 14, 2024 | Version 1.0 | Dotan Simha | Dotan Simha |

## APPENDIX A — Access management procedure

1. **Overview**
   This procedure outlines the process for managing access to company systems and resources, ensuring necessary access rights while maintaining security and compliance standards.
2. **Initiation and Standard Access Provisioning**
   Onboarding Completion: HR sends an email to the IT Service Desk upon completion of the employee onboarding process, generating service tickets for access.
   Provisioning Access: IT provisions access to all company-wide systems and engineering systems for Members of Technical Staff (MTS), including email, intranet, development environments, and collaboration tools.
3. **Requesting Additional Access**
   Access Request: Employees or managers submit requests for additional access through the IT Service Desk portal, including necessary details and justification.
   Approval Process: The request is reviewed and approved by the appropriate manager or system owner.
4. **Provisioning and Notification of Approved Access**
   Provisioning: IT provisions the approved access and updates the service ticket.
   Notification: IT notifies the employee and manager of the granted access, including any conditions or limitations.
5. **Access Review and Revocation**
   Periodic Review: IT conducts periodic reviews to ensure access is still required and appropriate.
   Revocation: When an employee changes roles or leaves the company, HR notifies IT to revoke access, updating the service tickets accordingly.

## APPENDIX B — Access matrix

| Role | Email | Google Workspace | Azure | GitHub | Notion | CloudFlare | Grafana |
|---|---|---|---|---|---|---|---|
| Open Source Developer | x | x | | x | x | x | |
| Hive Developer | x | x | | x | x | | |
| Hive Production Team | x | x | x | x | x | x | x |