∇inai

Access Control Policy

Version 1 - Approved by Shreyas Srinivas

Contents

1. Objective

The objective of this policy is to provide a framework to ensure that access to Inai Technologies Co assets is provided in a controlled manner based on business and information security requirements.

The framework is designed to ensure that appropriate controls for access management are established to protect Inai Technologies Co assets from security threats arising from unauthorized access.

2. Scope

This policy applies to specific systems that, from an access standpoint, have significant implications on Inai Technologies Co's ability to render its service commitments and safeguard information.

3. Policy Statement

Centralized access control is key to ensuring that the correct Inai Technologies Co staff members access the correct data and systems at the correct level. The principle of least privilege guides Inai Technologies Co's access controls. These controls apply to information and information processing systems at the application and operating system layers, including networks and network services.

The confidentiality, integrity, and availability of information stored within the information system of Inai Technologies Co shall be assured by ensuring that only authorized users have access to specific information assets as needed for their business activities.

4. Access Control Policy

4.1 Requirement for Access Control

- Every organization possesses information and information assets that need to be protected from unauthorized use.
- A list of critical systems within Inai Technologies Co that host services or sensitive data as defined in the scope of this document shall be identified and documented.
- It is the responsibility of the Information Security Officer to ensure all such systems used to meet business requirements at Inai Technologies Co are identified, and the list of critical systems is kept updated.

4.2 Access Management

4.2.1 Access Provisioning

- Inai Technologies Co shall provide access privileges to its systems based on the following principles:
  - Need to know – users or resources shall be granted access to systems that are necessary to fulfill their roles and responsibilities.
  - Least privilege – users or resources shall be given minimum privileges necessary to fulfill their roles and responsibilities.
  - Separation of duties – the practice of ensuring responsibility to perform critical actions is distributed among different individuals to keep a single individual from subverting the process.
- The minimum requirements for access control are to be achieved using one or both of the following methodologies:
  - Role-based Access control: This methodology restricts access to systems and resources based on individuals or groups with defined business functions -- e.g., executive level, engineer level 1, etc. -- rather than the identities of individual users.
  - Rule-based access control: This involves a formal registration and de-registration process for individual users where access is provided based on requests and approvals from authorized personnel.
- For Role-based access Control:
  - Access to information systems and services is restricted based on the role assigned to staff members.
  - The roles that may access each critical system shall be identified and documented.
  - By default, staff members are granted access to systems according to their role or team. The ability to grant access to systems is restricted to the administrators of each system.
  - If any access is required outside the defined role matrix, the business justification for such an event must be documented.
- For Rule-based/ Ticket-Based access control:
  - Requests for users' accounts and access privileges must be formally documented and appropriately approved. Access authorization information for a user must be retained for a minimum amount of time as defined in business, contractual, and legal requirements.
  - For any staff member requiring access to systems/platforms/tools, a request needs to be submitted detailing the specific access being requested.
  - The Acceptable Usage Policy needs to be accepted by an employee before being granted access to systems that contain customer data. This policy outlines responsibilities and commitments regarding the acceptable use of the Inai Technologies Co's assets.
  - If a Inai Technologies Co staff member requires access outside of the default for their role or team, either they or their managers may request additional access to the administrators of the respective systems.

- When granting such access, it shall be limited to the minimum level required to perform the intended business operation.

4.2.2 Management of Privileged Access Rights

- Inai Technologies Co operates its access management under the principle of least privilege.
- Under the principle of least privilege, a staff member should only be granted the minimum necessary access to perform their function. Access is considered necessary only when a Inai Technologies Co staff member cannot perform a function or action without that access. If an action can be performed without the requested access, it's not considered necessary. The least privilege is important because it protects Inai Technologies Co and its customers from unauthorized access and configuration changes and in case of an account compromise by limiting access.

4.2.3 Management of Passwords and Secret Authentication Information of Users

- It is recommended to minimize the use of passwords wherever possible. Please follow the guidelines to reduce the reliance on passwords:
  - Use a single-sign-on mechanism to authenticate yourself wherever possible. This avoids the need to create new strong passwords. Please ensure that the password/authentication mechanism for the SSO system is secure
  - Use multi-factor authentication (MFA) techniques to authenticate yourself wherever possible. This adds an additional barrier even if the password is compromised
- Where passwords are the only way to login to a system, it is recommended to consider the below security requirements:
  - Staff members must use complex passwords, wherever possible, for all of their accounts that have access to critical data. A strong password should consist of at least 8 characters and should contain a combination of alphanumeric + special characters
  - It is strongly recommended against the reuse of passwords that are or were used elsewhere, e.g., passwords used for personal accounts. A common way attackers obtain access to corporate resources is by using employees' personal passwords that were obtained in breaches of other services
- Inai Technologies Co shall ensure that any password or authentication details stored within systems owned and managed by Inai Technologies Co should be encrypted or masked to avoid exposing such details

4.2.4 Review of Access Rights

- There shall be a periodic reconciliation of user accounts and the associated rights. The reconciliation needs to be performed at least annually.
- Review of access rights must also include a review of privileges assigned to users.
- It is essential that appropriate actions are taken immediately to remove, disable or modify any irregularities found in the access reconciliation.

4.2.5 Removal or Adjustment of Access Rights

- Employment termination or change of roles shall trigger relevant processes for revoking or amending access rights.
- If there is a role change, necessary changes/adjustments shall be made so that the user does not have more rights than required to carry out the new job function.
- The removal or modification of access rights for terminated Inai Technologies Co employees or contract staff shall be carried out by the relevant administrators.

4.2.6 Secure Log-On Procedures

- Following shall be considered for security when accessing critical systems:
  - If the login is unsuccessful, the error message shall not display which part of the login information was incorrect.
  - Limit the number of unsuccessful log-on attempts.
  - Password shall not be displayed while it is being entered.
  - Multi-factor authentication shall be adopted wherever possible.
  - Using an authentication mechanism like single sign-on (SSO) is also recommended wherever possible.
- Session Time-Out
  - Inactive sessions (Application sessions, Administration Sessions, etc.) shall be shut down where feasible after a defined period of inactivity.
  - Intranet site may be exempted from the requirement of session time-out.
  - Session time-out requirements shall be implemented for all the critical systems as feasible and applicable.
  - Re-authentication may be considered at timed intervals.

4.2.7 Access Monitoring

- For all production infrastructure, logging must be enabled to ensure user accountability is maintained in case of any issues. It is recommended to have additional security measures like an intrusion detection/prevention system to detect any unauthorized access.

5. Document Security Classification

Company Internal (please refer to the Data Classification policy for details).

6. Non-Compliance

Compliance with this policy shall be verified through various methods, including but not limited to automated reporting, audits, and feedback to the policy owner. Any staff member found to be in violation of this policy may be subject to disciplinary action, up to and including termination of employment or contractual agreement. The disciplinary action shall depend on the extent, intent, and repercussions of the specific violation.

7. Responsibilities

The Information Security Officer is responsible for approving and reviewing policy and related procedures. Supporting functions, departments, and staff members shall be responsible for implementing the relevant sections of the policy in their area of operation.

8. Schedule

This document shall be reviewed annually and whenever significant changes occur in the organization.

End of Access Control Policy. For version history, please see the next page.

Version history

Version	Log	Date
1 Current	Policy version approved by Shreyas Srinivas	12 Mar, 2024
1	New Policy version Created	12 Mar, 2024