#  Access Control Policy

Version [Revision #]

Last modified: [Last modified date]

Last reviewed: [Last reviewed date]

Last Approval: [Last approval date]

#### *Disclaimer*

*This policy template is created as a useful resource. However, organizations remain fully responsible for the content of their policies. Every organization is unique, and the content and format of this template must be revised to meet your organization’s specific requirements. The set of templates available from Hyperproof is not exhaustive nor inclusive; your organization may choose to use only a portion of them or to split them into multiple policies. Do not rely on this policy template to meet legal, regulatory, or contractual requirements. Review your policy in detail to ensure that it is appropriately tailored to your organization's business objectives.*

### Security boundary under scope

1. [List of applicable systems]

### References

1. NIST 800-63:<https://pages.nist.gov/800-63-3/>
2. ISO/IEC 24760:<https://www.iso.org/standard/77582.html>
3. GDPR Articles 5, 6, 20
4. ISO/IEC 27001:2022: A.5.15, A.5.16, A.5.18, A.5.34, A.6.7, A.7.2, A.7.3, A.7.6, A.8.2, A.8.21, A.8.31
5. NIST 800-53 rev. 5: AC-1, AC-3, AC-6, AC-6(1), AC-6(2), AC-6(7), AC-6(9), AC-6(10), AC-17, AC-17(3), AC-17(4), AU-9(4), CM-5(1), CM-5(5), IA-8(4), SC-7, SC-7(3), SC-7(5), SC-7(7), SC-39
6. CIS v8: 3.3, 6.1, 6.7, 6.8, 16.8
7. PCI DSS 4.0: 1.2.8, 1.3.1, 1.3.3, 1.4.2, 7.1.1, 7.1.2, 7.2.1, 7.2.2, 7.2.4, 7.2.5.1, 7.2.3, 7.2.5, 7.3.1, 7.3.2, 7.3.3, 9.2.1, 9.3.1, 9.3.1.1
8. AICPA SOC 2 TSC: C1.1, CC6.1, CC6.2, CC6.3, CC6.7, CC8.1, P5.1, P5.2, P7.1

## Document ownership

 <(Choose from)>

* 1. Policy Owner:
		1. [Owner name] ([Owner email]), [Owner title]
	2. Information Security Officer:
		1. [Information officer name], ([Information officer email]), [Information officer title]
	3. System Owner(s):
		1. [System owner name], ([System owner email]), [System owner title]
	4. Process and Operational Owner(s)
		1. [process owner], ([process owner email]), [process owner title]
	5. System Administrator(s):
		1. [System admin name], ([System admin email]), [System admin title]
	6. Required Dissemination: <(Choose from)>
		1. IT Administrator
		2. Engineering
		3. Product Management
		4. Support
		5. Information Security Team
		6. [Organization name] Leadership Team
		7. Contractors
		8. Vendors
		9. Company Wide
		10. [Organization name] SIRT
	7. Optional Dissemination: <(Choose from)>
		1. IT Administrator
		2. Engineering
		3. Product Management
		4. Support
		5. Information Security Team
		6. [Organization name] Leadership Team
		7. Contractors
		8. Vendors
		9. Company Wide
		10. [Organization name] SIRT

## Purpose

The purpose of this Access Control Policy is to establish the framework for managing and controlling access to the organization's information systems, networks, physical locations, and data. This policy aims to ensure that access is granted based on the principles of least privilege and need-to-know, thereby protecting the confidentiality, integrity, and availability of the organization’s information assets. By defining the roles, responsibilities, and procedures related to access control, this policy seeks to prevent unauthorized access, mitigate security risks, and comply with relevant regulatory and legal requirements.

## Scope

This Access Control Policy applies to all employees, contractors, consultants, temporary staff, and any other individuals or entities who have access to the organization’s information systems, networks, physical locations, and data. It covers all organizational resources, including but not limited to:

* Information systems (e.g., servers, workstations, applications)
* Network infrastructure (e.g., routers, switches, wireless access points)
* Physical locations (e.g., data centers, offices, secure areas)
* Data (e.g., electronic records, databases, logs)
* Administrative tools and services (e.g., software, scripts)
* Remote access mechanisms (e.g., VPN, remote desktop)

The policy encompasses all aspects of access control, including user registration and de-registration, user access provisioning, privileged access, system and network access control, physical access control, data access and privacy, and audit and monitoring procedures related to access.

## Roles and responsibilities

<(choose from)>

| **Role** | **Person &/or Title** | **Responsibility** |
| --- | --- | --- |
| Plan and Policy Management | [Owner name], **[owner title]** | Establish the controls, implementation, and monitoring strategy for [policy topic] and associated policy and procedure |
| Executive Review | **Executive Team** | Adjusts [policy topic] parameters to meet business requirements and appropriate risk appetite. Approves risk model and supporting risk documentation that applies to the [policy topic] Policy. Reads, understands and approves after appropriate editing, the [policy topic] Policy. |
| Approval and Commitment | **Executive Team** | Responsible for approval, and commitment to information security controls. Members of the leadership team of [Organization] to include [list of executive approvers]. |
| Information System Owner | [Information officer name], **[Information officer title]** | Responsible for the overall implementation, development, integration, modification, or operation and maintenance of configuration management. Develops operational strategies and tactics to comply with configuration management policy in coordination with the information systems administrators, the information security officer, and functional “end users.” |
| Operations | [Operational owner], **Operational owner title]** |  |
| Information Systems Administrators | **System Administrators**  | Effectively manages the daily implementation, monitoring, and maintenance of operational security controls, as directed by the System Owner and Information Security Officer. |
| Human Resource | [HR name], **[HR title]** | Setups HR wellbeing strategies, coordinates travel policy across the organization. Initiates emergency travel considerations, including crisis management when required. |
| End Users |  **End Users** | Users of information systems are required to comply with policy and procedures in the [policy topic] policy. |
| Providers | **[provider type]** | [provider service description] |

## Management commitment

* 1. [Organization] executive management affirms its commitment to the establishment, implementation, resourcing, monitoring, and effectiveness of [policy topic] controls and policy
	2. Management has reviewed and approved this policy.
	3. This policy demonstrates management's commitment to maintaining adequate controls as part of its information security management and privacy objectives. These objectives include compliance with applicable laws, regulatory requirements, executive orders, industry best practices, standards, guidelines, and contractual commitments.
	4. Management agrees to regularly review and update this policy to ensure that it effectively meets the organization’s business and compliance objectives.

## Coordination among organizational entities

1. The [responsible group] creates policy and procedure and is responsible for overall configuration management.
2. Policy and procedures will be reviewed, modified, and disseminated to required consumers.
3. The [responsible group] is responsible for coordinating documentation review and updating the policy.
4. The [responsible group] is responsible for communicating the policy and procedures to applicable required and optional parties.
5. The [responsible group] is responsible for training applicable required and optional parties on compliance with the policy and procedures.

## Compliance

* 1. Employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties.
	2. Non-employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to IT resources, and other actions as well as both civil and criminal penalties

## Definitions

* 1. Access Control:
		1. Measures and controls that ensure access to assets is authorized and restricted based on business and security requirements.
	2. User Registration and De-registration:
		1. Formal procedures for adding new users and removing users who no longer require access to the organization’s systems, networks, or data.
	3. Least Privilege:
		1. A security principle whereby users are granted the minimum levels of access – or permissions – needed to perform their job functions.
	4. Access Provisioning:
		1. The process of granting or denying specific access requests to information systems or data.
	5. Access Reviews:
		1. Regular evaluations of user access rights to ensure that they are appropriate and necessary for current job functions.
	6. Network Segmentation:
		1. The practice of splitting a computer network into subnetworks, each being a network segment, to enhance security and performance.
	7. Virtual Private Network (VPN):
		1. A technology that creates a safe and encrypted connection over a less secure network, such as the internet.
	8. Role-Based Access Control (RBAC):
		1. An approach to restricting system access to authorized users based on their role within an organization.
	9. Session Management:
		1. Procedures and technologies used to manage and secure the duration of a user's connection to a network or system.
	10. Audit and Monitoring:
		1. The process of recording and examining activity in information systems to ensure compliance with policies and to detect and respond to unauthorized activities.
	11. Physical Access Control:
		1. Measures that control the physical access to secure areas within an organization, including buildings and rooms.
	12. Secure Areas:
		1. Designated locations where sensitive information is processed or stored, requiring controlled access.
	13. Visitor Management:
		1. Procedures for monitoring and managing visitors to an organization’s facilities to ensure they do not access secure areas without authorization.
	14. Data Protection Officer:
		1. A designated individual responsible for overseeing data protection strategy and implementation to ensure compliance with regulatory requirements.
	15. Logs and Records:
		1. Documentation of system activities and user interactions, used for auditing and monitoring purposes.
	16. Personal Data:
		1. Information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, by reference to an identifier such as a name, identification number, location data, or an online identifier.
	17. Administrative Software, Scripts, and Services:
		1. Tools and programs used by IT administrators to manage, configure, and maintain computer systems and networks.
	18. Environment:
		1. The set of hardware, software, network resources, and services that make up the infrastructure where applications run and data is processed and stored.
	19. Protected Information:
		1. Data that is classified and requires measures to ensure its confidentiality, integrity, and availability are preserved.

## Policy

#### User Access Management

The [responsible party] shall:

##### User Registration and De-registration

* + - 1. Maintain formal procedures for the registration and de-registration of users.
			2. Ensure that access to information, services, systems, and documents is granted based on the principle of least privilege and authorized approval.
			3. Implement timely de-registration of users and revocation of access rights upon termination or role change.

##### User Access Provisioning

* + - 1. Implement a robust access provisioning process, ensuring access rights are assigned based on the principle of least privilege and need-to-know basis.
			2. Ensure that privileged access rights are strictly controlled and limited to authorized personnel only.

##### Access Reviews

* + - 1. Conduct quarterly access reviews to ensure user access rights remain appropriate and justified.
			2. Revoke access immediately upon user termination or change in role that no longer justifies the same level of access.

#### Network Access Control

The [responsible party] shall:

##### Policy on Use of Network Services

* + - 1. Ensure that only authorized users can access the network and network services based on least privilege.
			2. Use network segmentation to restrict access to sensitive information and systems.
			3. Implement intrusion detection and prevention systems (IDPS) to monitor and protect network traffic.

##### Remote Access

* + - 1. Require secure remote access solutions, such as Virtual Private Networks (VPNs), for all remote connections.
			2. Ensure remote access connections are monitored and logged for auditing purposes.
			3. Implement time-of-day and location-based restrictions for remote access where feasible.

##### Wireless Access

* + - 1. Implement secure configurations for wireless access points (WAPs).
			2. Use strong encryption protocols (e.g., WPA3) to secure wireless communications.
			3. Regularly review and update wireless access security settings.

#### System Access Control

The [responsible party] shall:

##### Access to Systems, Services, and Documents

* + - 1. Restrict access to systems, services, and documents based on job roles and responsibilities, following the principle of least privilege.
			2. Implement role-based access control (RBAC) and ensure it is enforced consistently across all systems.
			3. Ensure that default system accounts are disabled or securely configured.

##### Access to Administrative Software, Scripts, and Services

* + - 1. Restrict access to administrative software, scripts, and services to authorized personnel only.
			2. Ensure that administrative access is granted based on least privilege and need-to-know principles.

##### Access to Environments, Databases, and Protected Information

* + - 1. Implement access controls to ensure that only authorized users can access environments, databases, and protected information.
			2. Regularly review access to these resources to ensure compliance with access control policies.

##### Session Management

* + - 1. Implement session timeouts for inactive sessions, with automatic logoff after 15 minutes of inactivity.
			2. Ensure secure session handling, including encryption of session data in transit and at rest.

##### Audit and Monitoring

* + - 1. Enable and configure system logging to record all access attempts, both successful and unsuccessful.
			2. Regularly review access logs and system audit trails to identify and respond to unauthorized access attempts.

#### Physical Access Control

The [responsible party] shall:

##### Secure Areas

* + - 1. Designate secure areas where sensitive information is processed or stored.
			2. Implement physical access controls, such as card access systems, to restrict entry to secure areas.
			3. Ensure that access to secure areas is logged and regularly reviewed.

##### Visitor Management

* + - 1. Require visitors to sign in and out and be escorted while in secure areas.
			2. Issue temporary access badges for visitors and ensure they are collected upon departure.

#### Data Access and Privacy

The [responsible party] shall:

##### Access to Logs and Records

* + - 1. Restrict access to logs and records to authorized personnel only, based on least privilege principles.
			2. Ensure that logs and records are protected from unauthorized access and tampering.

##### Access to Personal Data

* + - 1. Allow users access to their personal data upon request, in accordance with data protection regulations.
			2. Implement procedures to verify user identity before granting access to personal data.

## Policy exemptions

* 1. Requests for exceptions to this policy shall be reviewed by the [exemption officer 1] and the [exemption officer 2] and/or the [responsible group].
	2. Employees requesting exceptions shall provide such requests to [exemption communication channel].
	3. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the [responsible group], initiatives, actions, and a timeframe for achieving the minimum compliance level with the policies set forth herein.

## Related documents

* 1. [list of related documents, including:
		1. Policies
		2. Procedures
		3. Standards
		4. Documentation
		5. Regulations
		6. Legal context

]

## Revision history

* 1. This policy is reviewed and, if necessary, updated annually and may also be updated to reflect changes in the environment.
	2. Every change to this plan must be reviewed and evidence of review and acceptance noted with a signature below. This plan requires the signature of: <(choose from)>
		1. The Information Security Officer
		2. Officer of the [Organization name] Leadership Team
	3. All changes requiring approval must be communicated to the required parties

| **Rev. #** | **Revision Date** | **Description** | **Author** | **Owner** | **Exec. reviewer** |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |

## Approval history

| **Step** | **Approver** | **Job Function** | **Signature** | **Approval Date** |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |