# Acceptable Use 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 and legal requirements.*

### Security boundary under scope

1. [List of applicable systems]

### References

1. ISO/IEC 27001:2022: A.5.10
2. NIST 800-53 rev. 5: CM-10, CM-11
3. PCI DSS 4.0: 12.2.1
4. AICPA SOC 2 TSC: CC6.8

## 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 the Acceptable Use Policy is to establish guidelines and define acceptable behavior for users when accessing and using [Organization]'s information systems and resources. This policy aims to protect the security, integrity, and availability of these systems and data, ensure compliance with legal and regulatory requirements, and safeguard the interests of [Organization] and its stakeholders.

## Scope

This Acceptable Use Policy applies to all employees, contractors, consultants, temporary staff, and other individuals who are authorized to access and use [Organization]'s information systems and resources. This includes, but is not limited to, all computer systems, networks, applications, data, and communication devices owned or managed by [Organization]. The policy covers all activities conducted on [Organization]'s systems, whether performed on-site or remotely, and applies to both business and limited personal use of organizational resources.

## 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. Authorized Access
	1. Permission granted to users to enter or use information systems and resources, ensuring they have the necessary rights and privileges.
2. Encryption
	1. A method of converting information or data into a code, especially to prevent unauthorized access.
3. Malware
	1. Software designed to disrupt, damage, or gain unauthorized access to computer systems.
4. Network
	1. A group of interconnected computers and devices that share resources and information.
5. Sensitive Data
	1. Information that requires protection due to its confidential nature, such as personal, financial, or health data.
6. Software Licensing Agreement
	1. A legal contract between the software developer and the user, outlining the terms under which the software can be used.
7. Unauthorized Access
	1. Access to information systems and data without permission, often resulting in security breaches or data theft.
8. User ID and Password
	1. Unique identifiers used by individuals to authenticate their identity and gain access to information systems.
9. User
	1. An individual who is authorized to use the organization's information systems and resources.
10. Virus
	1. A type of malware that, when executed, replicates itself by modifying other computer programs and inserting its own code.
11. Data Classification Standards
	1. Guidelines for categorizing data based on its level of sensitivity and the impact that its disclosure, modification, or destruction would have on the organization.
12. Data Retention and Destruction Policies
	1. Organizational rules and procedures for maintaining, storing, and securely disposing of data after it is no longer needed.
13. Phishing
	1. A cyber attack method where attackers send fraudulent messages designed to trick individuals into revealing sensitive information.
14. Incident Reporting
	1. The process of notifying the relevant authorities or departments within an organization about a security breach or violation of policies.

## Policy

#### General Guidelines

All users of [Organization]'s information systems and resources are required to adhere to the following guidelines to ensure security, integrity, and availability of these assets:

##### Compliance with Laws and Regulations

* + - 1. Users shall comply with all applicable local, state, federal, and international laws, as well as organizational policies and procedures.
			2. Users are required to avoid any activity that could result in a violation of these laws and regulations.

##### Authorized Use

* + - 1. Access to [Organization]'s systems and data is restricted to authorized users only.
			2. Users shall only access data and systems for which they have explicit authorization.
			3. Users are required to use their assigned user IDs and passwords and shall not share their credentials with others.

##### System and Data Protection

* + - 1. Users shall ensure that their actions do not compromise the security of information systems and data.
			2. Users are required to use encryption methods approved by [Organization] when transmitting sensitive data.
			3. Users shall immediately report any suspicious activities or security incidents to the [Information Security Team/Helpdesk].

##### Internet and Email Use

* + - 1. Internet access provided by [Organization] is intended for business purposes. Limited personal use is permitted as long as it does not interfere with job responsibilities and complies with this policy.
			2. Users shall not use [Organization]’s email systems to transmit unauthorized, illegal, or offensive content.
			3. Users are required to avoid opening email attachments or clicking on links from unknown or untrusted sources.

##### Software and Hardware Use

* + - 1. Users shall only install and use software that is authorized and licensed by [Organization].
			2. Users are required to adhere to software licensing agreements and shall not use unlicensed or pirated software.
			3. Users shall not connect unauthorized devices to [Organization]'s network without prior approval from the [IT Department].

##### Data Handling

* + - 1. Users shall classify, handle, and protect information according to [Organization]'s data classification standards.
			2. Users are required to securely store and dispose of sensitive information in accordance with [Organization]'s data retention and destruction policies.

#### Prohibited Activities

Users of [Organization]'s information systems and resources are strictly prohibited from engaging in the following activities:

##### Unauthorized Access and Use

* + - 1. Users shall not attempt to gain unauthorized access to any system, network, or data.
			2. Users are prohibited from using another user’s credentials to access [Organization]’s systems.

##### Malicious Activities

* + - 1. Users shall not engage in activities that may harm or disrupt [Organization]’s systems, such as introducing malware, viruses, or other harmful software.
			2. Users are prohibited from engaging in activities that could be considered hacking or exploiting vulnerabilities in [Organization]'s systems.

##### Misuse of Resources

* + - 1. Users shall not use [Organization]’s resources for personal financial gain, commercial activities, or political campaigns.
			2. Users are prohibited from using [Organization]’s resources to access, create, or distribute inappropriate or offensive content.

##### Privacy Violations

* + - 1. Users shall respect the privacy and confidentiality of others and shall not access, read, or distribute another user’s personal information without authorization.
			2. Users are prohibited from capturing or monitoring network traffic, except when authorized for legitimate business purposes.

## 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** |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |