[Organization Name]

Acceptable Use Policy

POL-002

Version 1.0
[Effective Date]

Classification: Internal Use

Document Owner	Chief Information Security Officer
Approved By	Chief Executive Officer
Review Frequency	Annual or upon significant change

Table of Contents

1. Introduction and Purpose 4
1.1 Introduction 4
1.2 Purpose 4
1.3 Policy Statement 5
2. Scope 5
2.1 Organisational Scope 5
2.2 Personnel Scope 5
2.3 Systems Scope 6
2.4 Exclusions 6
3. Definitions and Terminology 6
3.1 General Terms 6
3.2 Technical Terms 7
4. Related Documents 7
4.1 Parent Policy 7
4.2 Supporting Policies 8
4.3 Supporting Standards 8
4.4 Supporting Processes 8
4.5 Document Availability 8
5. Acceptable Use Requirements 9
5.1 General Principles 9
5.2 Acceptable Use 9
5.3 Unacceptable Use 9
5.4 Email and Communications 10
5.5 Internet Use 10
5.6 Social Media 11
5.7 Mobile Devices 11
5.8 AI and Automated Tools 11
5.9 Software and Applications 12
5.10 Data Handling 12
6. Monitoring and Privacy 12
6.1 Monitoring Rights 12
6.2 Privacy Expectations 12
6.3 Audit and Investigation 13
7. Roles and Responsibilities 13
7.1 All Personnel 13
7.2 Managers and Supervisors 13
7.3 IT Department 14

7.4 Information Security Team 14
7.5 Human Resources 14
8. Compliance and Enforcement 14
8.1 Compliance Requirements 14
8.2 Violations and Consequences 14
8.3 Reporting Violations 15
9. Policy Exceptions 15
9.1 Exception Process 15
9.2 Exception Approval 15
9.3 Exception Documentation 16
10. Document Control 16
10.1 Document Information 16
10.2 Revision History 16
10.3 Approval Signatures 16
Appendix A: Acceptable Use Acknowledgment Form 16

1. Introduction and Purpose

1.1 Introduction

This Acceptable Use Policy establishes comprehensive requirements and expectations for the appropriate use of [Organization Name]'s information systems, technology resources, and data assets. The policy applies to all personnel who access organizational systems and is designed to protect both the organization and its personnel from security risks, legal liability, and operational disruption arising from inappropriate use of technology resources.

Information systems and technology resources are essential tools that enable [Organization Name] to conduct business operations effectively, serve customers, and achieve strategic objectives. These resources represent significant organizational investment in infrastructure, software, and support services. Protecting these resources from misuse, abuse, and security threats is essential for maintaining operational capability and stakeholder trust.

The proliferation of digital technologies, cloud services, mobile devices, and artificial intelligence tools has expanded the scope and complexity of acceptable use considerations. This policy provides a comprehensive framework that addresses both traditional and emerging technology use scenarios while remaining flexible enough to accommodate evolving business needs and technological change.

This policy operates under and complements the Information Security Policy (POL-001), which establishes the overarching framework for information security governance within [Organization Name]. Where requirements in this policy overlap with or extend requirements in other organizational policies, this policy shall be read in conjunction with those policies, with the most restrictive requirement applying in cases of conflict.

1.2 Purpose

The purpose of this policy is to establish clear, comprehensive expectations for the acceptable use of organizational information systems and technology resources. Specifically, this policy aims to:

Define what constitutes acceptable and unacceptable use of organizational systems, providing personnel with clear guidance on expected behavior and boundaries. This clarity enables personnel to make informed decisions about technology use and reduces uncertainty about what is permitted.

Protect the organization from legal liability arising from inappropriate system use, including liability related to intellectual property infringement, defamation, harassment, privacy violations, and regulatory non-compliance. Clear policies and documented acknowledgment help establish that the organization has taken reasonable steps to prevent misuse.

Protect personnel by establishing clear boundaries and expectations, ensuring that all users understand their responsibilities and the consequences of policy violations. This protection extends to both the individual user and their colleagues who may be affected by inappropriate use.

Ensure the security, integrity, and availability of information systems by preventing activities that could compromise system security, corrupt data, consume excessive resources, or disrupt operations. Acceptable use policies are a fundamental control in any information security programme.

Support compliance with legal, regulatory, and contractual obligations by establishing controls that address requirements related to data protection, privacy, record retention, and industry-specific regulations. Many compliance frameworks require documented acceptable use policies.

Preserve organizational reputation and stakeholder trust by preventing activities that could embarrass the organization, damage relationships with customers or partners, or undermine public confidence in the organization's professionalism and integrity.

1.3 Policy Statement

[Organization Name] provides information systems and technology resources to personnel for legitimate business purposes. These resources are organizational assets that must be used responsibly, professionally, and in accordance with this policy and all applicable laws and regulations.

Personnel are expected to exercise good judgment when using organizational systems. When the appropriateness of a particular use is unclear, personnel should seek guidance from their manager or the Information Security team before proceeding. The principle of 'when in doubt, ask' should guide decision-making.

The organization reserves the right to monitor the use of its information systems and technology resources to ensure compliance with this policy, protect organizational assets, investigate security incidents, and meet legal and regulatory requirements. Personnel should have no expectation of privacy when using organizational systems.

Violations of this policy may result in disciplinary action up to and including termination of employment or contract, as well as potential civil or criminal liability for illegal activities. The organization will enforce this policy consistently and fairly across all personnel.

2. Scope

2.1 Organizational Scope

This policy applies to all business units, departments, functions, and locations of [Organisation Name], including headquarters, branch offices, remote work locations, and any other sites where organizational technology resources are used. The policy applies equally to domestic and international operations.

Subsidiaries, controlled entities, and joint ventures where [Organization Name] has management control shall adopt this policy or implement equivalent acceptable use controls. Where [Organization Name] participates in partnerships or joint ventures without management control, this policy shall apply to [Organization Name] personnel and systems within those arrangements.

2.2 Personnel Scope

This policy applies to all individuals who access [Organisation Name]'s information systems and technology resources, regardless of their employment status or relationship with the organization. This includes:

- Employees at all levels, including executives, managers, professional staff, administrative staff, and operational personnel. No employee is exempt from this policy by virtue of their position or seniority.
- Contractors, consultants, and temporary workers engaged by the organization, whether working on-site or remotely. Contractual agreements with these parties shall reference compliance with this policy.
- Third-party service providers, vendors, and partners who are granted access to organizational systems. Access agreements shall include acceptable use provisions consistent with this policy.

Interns, volunteers, and any other individuals authorized to use organizational technology resources for any purpose.

2.3 Systems Scope

This policy applies to all information systems and technology resources owned, leased, licensed, or operated by [Organization Name], regardless of where they are located or how they are accessed. This includes:

- Computer hardware, including servers, desktop computers, laptop computers, tablets, and any other computing devices provided by the organization or used to access organizational resources.
- Network infrastructure, including local area networks, wide area networks, wireless networks, virtual private networks, firewalls, routers, switches, and related equipment.
- Software and applications, including operating systems, productivity software, business applications, cloud services, and any other software licensed or developed by the organization.
- Communication systems include email, instant messaging, video conferencing, telephony, and collaboration platforms.
- Data and information assets, including databases, file shares, documents, records, and any other data created, processed, stored, or transmitted using organizational systems.
- Mobile devices including smartphones, tablets, and wearable devices, whether organization-owned or personal devices used to access organizational resources.
- Cloud services and external platforms accessed using organizational credentials or for organizational purposes, including software-as-a-service, platform-as-a-service, and infrastructure-as-a-service offerings.

2.4 Exclusions

This policy does not apply to personal devices and services used exclusively for personal purposes with no connection to organizational systems, data, or business activities. However, if personal devices are used to access organizational resources, the provisions of this policy apply to that use.

This policy does not govern the internal operations of third-party service providers except to the extent that they access organizational systems. Third-party security requirements are addressed in the Third-Party Security Policy (POL-011) and associated contracts.

3. Definitions and Terminology

3.1 General Terms

Term	Definition
Information Systems	All computer hardware, software, networks, and related technology infrastructure owned, leased, or operated by the organization for processing, storing, or transmitting information.
Technology Resources	Computing equipment, software applications, network services, cloud platforms, and related infrastructure

	provided by the organization to support business operations.
Authorized User	An individual who has been granted formal permission to access organizational systems through established authorization processes and who has acknowledged applicable policies.
Business Purpose	Activities that directly support or are reasonably related to the user's job responsibilities, organizational objectives, or legitimate operational needs.
Personal Use	Use of organizational systems for purposes unrelated to job responsibilities or organizational business, including personal communications, entertainment, and private affairs.
Sensitive Information	Data that requires protection due to its confidential, proprietary, personal, or regulated nature, including but not limited to personal data, financial information, and trade secrets.

3.2 Technical Terms

Term	Definition
Malware	Malicious software designed to damage, disrupt, or gain unauthorized access to computer systems, including viruses, worms, trojans, ransomware, and spyware.
Phishing	Fraudulent attempts to obtain sensitive information by disguising communications as trustworthy sources, typically through deceptive emails, websites, or messages.
Shadow IT	Technology systems, software, or services used within the organization without explicit approval or oversight from IT or Information Security.
Multi-Factor Authentication	An authentication method requiring two or more verification factors to gain access, typically combining something you know, have, or are.
Encryption	The process of converting information into a coded format that can only be read by authorized parties possessing the appropriate decryption key.

4. Related Documents

4.1 Parent Policy

This policy operates under the Information Security Policy (POL-001), which establishes the overarching framework for information security governance within [Organization Name]. All requirements in this policy shall be interpreted consistently with POL-001.

4.2 Supporting Policies

The following policies provide additional requirements that complement and extend this Acceptable Use Policy:

Document ID	Document Title	Relevance
POL-003	Access Control Policy	User authentication and authorization requirements
POL-004	Data Protection and Privacy Policy	Personal data handling and privacy requirements
POL-013	Network Security Policy	Network access and security requirements
POL-018	Cloud Security Policy	Cloud service usage requirements
POL-019	AI Security Policy	AI and automated tool usage requirements
POL-021	Remote Access Policy	Remote and mobile access requirements

4.3 Supporting Standards

Document ID	Document Title	Relevance
STD-001	Password and Authentication Standard	Password requirements and authentication controls
STD-003	Data Classification Standard	Data handling based on classification level
STD-006	Endpoint Security Standard	Device security configuration requirements
STD-013	Mobile Device Security Standard	Mobile device usage and security requirements

4.4 Supporting Processes

Document ID	Document Title	Relevance
PRC-003	Security Exception Process	Process for requesting policy exceptions
PRC-005	Incident Management Process	Reporting and handling security incidents

4.5 Document Availability

All supporting documentation referenced in this policy is available through the organization's document management system. Personnel shall ensure they have access to and are familiar with current versions of relevant documentation. The Information Security team maintains authoritative versions of all security documentation.

5. Acceptable Use Requirements

5.1 General Principles

Personnel shall use organizational information systems and technology resources primarily for legitimate business purposes that support their job responsibilities and organizational objectives. All use shall comply with applicable laws, regulations, contractual obligations, and organizational policies.

Personnel are individually accountable for all activities conducted under their user accounts and credentials. Sharing of credentials, passwords, or access tokens with others is strictly prohibited, regardless of the relationship between the parties or the business justification offered.

Personnel shall protect their credentials from disclosure and shall not write down passwords, store them in unsecured locations, or transmit them through insecure channels. Any suspected compromise of credentials shall be reported immediately to the IT Service Desk.

When the appropriateness of a particular use is unclear, personnel should apply the 'front page test': would this activity be appropriate if reported on the front page of a newspaper? When in doubt, seek guidance before proceeding.

5.2 Acceptable Use

The following uses of organizational systems are explicitly acceptable and encouraged:

- Performing job-related duties and responsibilities, including all activities necessary to fulfill one's role within the organization.
- Accessing, creating, processing, and storing information necessary for work functions, subject to data classification requirements and need-to-know principles.
- Communicating with colleagues, customers, partners, and other stakeholders for legitimate business purposes using approved communication channels.
- Participating in authorized training, professional development, and educational activities that support job performance or career growth.
- Researching work-related topics, industry developments, and professional knowledge using appropriate internet resources.

Limited personal use that is reasonable in duration and frequency, does not interfere with job performance, does not consume excessive resources, and does not violate any other provisions of this policy. Examples include brief personal email, occasional news reading, and similar de minimis activities.

5.3 Unacceptable Use

The following uses of organizational systems are strictly prohibited:

- Accessing, downloading, storing, or transmitting illegal content of any kind, including but not limited to pirated software, illegal media, and content depicting illegal activities.
- Engaging in harassment, discrimination, bullying, or any form of hostile or offensive communication, whether directed at colleagues, customers, or third parties.
- Attempting to gain unauthorized access to systems, data, or accounts, including using others' credentials, exploiting vulnerabilities, or bypassing security controls.
- Circumventing, disabling, or interfering with security controls, monitoring systems, or protective measures implemented by the organization.

- Installing, downloading, or using unauthorized software, applications, browser extensions, or cloud services without explicit approval from IT.
- Using organizational systems for personal commercial activities, side businesses, or any form of personal financial gain unrelated to organizational business.
- Excessive personal use that interferes with job duties, consumes significant bandwidth or storage, or distracts from work responsibilities.
- Accessing, viewing, downloading, or distributing pornographic, obscene, or sexually explicit material.
- Gambling, gaming, cryptocurrency mining, or participating in online betting or wagering activities.
- Sharing confidential, proprietary, or sensitive information without proper authorization and appropriate safeguards.
- Using organizational resources for political campaigning, lobbying, or advocacy unrelated to legitimate business interests.
- Impersonating others, falsifying identity, or misrepresenting one's role or authority.
- Any activity that could expose the organization to legal liability, reputational harm, or financial loss.

5.4 Email and Communications

Personnel shall use organizational email and communication systems professionally and responsibly. Email is a formal business communication channel and messages should be composed with appropriate care and consideration.

Email shall not be used for chain letters, spam, mass unsolicited messages, or personal distribution lists. Forwarding of jokes, memes, or non-business content to multiple recipients is discouraged.

Personnel shall exercise caution with attachments and links, particularly from unknown or unexpected sources. Suspicious emails shall be reported to IT Security rather than opened or forwarded.

Business communications should be professional in tone and content. Personnel should assume that any email could be read by unintended recipients, disclosed in litigation, or preserved indefinitely.

Auto-forwarding of organizational email to external accounts is prohibited without explicit approval. Out-of-office messages should not disclose sensitive information about travel or availability.

5.5 Internet Use

Internet access is provided to support business operations and should be used primarily for work-related purposes. Personnel may access the internet for work-related research, communication, transactions, and professional development.

Downloading files from the internet should be limited to legitimate business needs and should only occur from reputable sources. Executable files, scripts, and software shall not be downloaded without IT approval.

Streaming media, video conferencing, and high-bandwidth activities should not consume excessive network resources or interfere with business operations. Large downloads should be scheduled for off-peak hours where possible.

Access to inappropriate, illegal, offensive, or potentially harmful websites is prohibited. The organization may implement technical controls to block access to certain categories of websites.

Personnel shall not use anonymizing proxies, VPN services, or other tools to circumvent web filtering or monitoring controls without explicit authorization.

5.6 Social Media

Personnel shall not represent themselves as speaking on behalf of [Organization Name] on social media without explicit authorization from the Communications or Marketing department. Personal social media accounts should clearly indicate that views expressed are personal.

Confidential, proprietary, or sensitive information shall not be disclosed on social media platforms under any circumstances. This includes information about customers, partners, employees, and internal operations.

Personnel should be mindful that their social media activity, even on personal accounts, may reflect on the organization and could affect professional relationships. Conduct that would be inappropriate in the workplace is also inappropriate online.

Excessive social media use during work hours is discouraged and may be addressed as a performance issue. Social media should not interfere with job responsibilities or productivity.

5.7 Mobile Devices

Mobile devices used to access organizational systems, whether organization-owned or personal, shall be protected with appropriate security controls including device encryption, screen locks, and remote wipe capability.

Lost or stolen devices that have been used to access organizational systems shall be reported immediately to the IT Service Desk, regardless of whether the device is organization-owned or personal.

Personal devices used for work purposes (BYOD) must comply with the Mobile Device Security Standard (STD-013) and may be subject to security requirements including mobile device management software.

Organizational data shall not be stored on unapproved personal devices or transferred to personal cloud storage services. Data synchronization shall only use approved services and methods.

Mobile devices shall not be used while driving except with appropriate hands-free equipment and in compliance with applicable laws. Safety takes precedence over communication convenience.

5.8 AI and Automated Tools

Use of artificial intelligence tools, large language models, chatbots, and automated services shall comply with the AI Security Policy (POL-019) and any specific guidance issued by Information Security.

Confidential, proprietary, personal, or sensitive data shall not be input into external AI systems, chatbots, or automated tools that have not been explicitly approved for such use. This includes commercial AI services like ChatGPT, Claude, and similar tools unless specifically authorized.

AI-generated content shall be reviewed for accuracy, appropriateness, and potential intellectual property concerns before use in business contexts. Personnel remain accountable for work products regardless of AI assistance.

Automated tools shall not be used to circumvent security controls, generate misleading content, create deepfakes, or engage in any deceptive practices.

5.9 Software and Applications

Only software and applications approved by IT shall be installed on organizational systems. Requests for new software should be submitted through established IT request processes.

Browser extensions, plugins, and add-ons shall not be installed without IT approval, as these can introduce security vulnerabilities and privacy risks.

Cloud services and software-as-a-service applications shall not be used for organizational data without IT approval. Shadow IT creates security and compliance risks.

Software licences shall be respected at all times. Pirated, unlicensed, or improperly licensed software shall not be used on organizational systems.

5.10 Data Handling

Organizational data shall be handled in accordance with its classification level as defined in the Data Classification Standard (STD-003). More sensitive data requires more stringent protections.

Data shall not be copied to removable media, personal devices, or external services except where necessary for business purposes and in compliance with applicable policies.

When work involving sensitive data is complete, data should be properly secured or disposed of according to retention requirements. Sensitive documents should not be left unattended.

Data breaches, suspected data loss, or unauthorized data disclosure shall be reported immediately through incident reporting channels.

6. Monitoring and Privacy

6.1 Monitoring Rights

[Organization Name] reserves the right to monitor, log, audit, and inspect all use of its information systems and technology resources. This monitoring may occur without prior notice and may include:

- Network traffic analysis to detect security threats, policy violations, and performance issues.
- Email content inspection to identify malware, data leakage, and inappropriate communications.
- Internet usage logging to track website access patterns and identify potentially harmful activities.
- File access auditing to monitor who accesses what data and when.
- Application usage monitoring to understand software utilization and identify unauthorized tools.
- Keystroke logging and screen capture in specific circumstances where authorized for investigation purposes.

6.2 Privacy Expectations

Personnel should have no expectation of privacy when using organizational information systems and technology resources. All data stored on, processed by, or transmitted through

organizational systems may be accessed, reviewed, and disclosed by authorized personnel for legitimate purposes.

Personal files, emails, and communications stored on or transmitted through organizational systems are not private and may be accessed during investigations, audits, or legal proceedings.

The use of personal accounts, encrypted communications, or other means to conduct business on organizational systems does not create an expectation of privacy.

Personnel consent to monitoring by accepting employment or engagement with [Organization Name] and by acknowledging this policy.

6.3 Audit and Investigation

The organization may conduct audits of system usage to verify compliance with this policy and identify potential security issues. Audits may be conducted on a routine basis or in response to specific concerns.

In cases of suspected policy violations, security incidents, or legal matters, the organization may conduct detailed investigations of individual user activity. Such investigations will be conducted in accordance with applicable laws and HR policies.

Personnel shall cooperate fully with authorized audits and investigations, including providing access to devices, accounts, and information as required.

7. Roles and Responsibilities

7.1 All Personnel

All personnel who use organizational systems are responsible for:

- Reading, understanding, and complying with this policy and all related security policies, standards, and procedures.
- Using organizational systems responsibly, professionally, and ethically in accordance with this policy.
- Protecting credentials, access tokens, and authentication factors from disclosure or misuse.
- Reporting suspected policy violations, security incidents, or concerns through appropriate channels.
- Completing required security awareness training and staying current on security guidance.
- Seeking guidance when uncertain about whether a particular use is acceptable.
- Signing and complying with the Acceptable Use Acknowledgment Form.

7.2 Managers and Supervisors

Managers and supervisors have additional responsibilities including:

- Ensuring personnel under their supervision understand and comply with this policy.
- Addressing observed policy violations promptly and appropriately through HR processes.
- Modelling acceptable use behaviour and promoting a culture of security awareness.
- Escalating significant concerns or repeated violations to appropriate parties.

- Supporting investigations and audits as required.
- Ensuring new team members complete required acknowledgments and training.

7.3 IT Department

The IT Department is responsible for:

- Implementing and maintaining technical controls that support and enforce this policy.
- Monitoring systems for policy violations, security threats, and performance issues.
- Investigating reported incidents and suspected violations in coordination with Information Security and HR.
- Maintaining and updating acceptable use guidelines and user documentation.
- Providing guidance and support to personnel on acceptable use questions.
- Managing the software approval process and maintaining the approved software list.

7.4 Information Security Team

The Information Security Team is responsible for:

- Maintaining this policy and ensuring it remains current and effective.
- Defining security requirements that inform acceptable use standards.
- Reviewing exception requests and making risk-based recommendations.
- Conducting security awareness training related to acceptable use.
- Coordinating investigation of significant security incidents related to policy violations.

7.5 Human Resources

Human Resources is responsible for:

- Ensuring this policy is communicated to all personnel during onboarding.
- Maintaining records of policy acknowledgments.
- Managing disciplinary processes for policy violations in accordance with employment policies.
- Supporting managers in addressing performance issues related to policy violations.

8. Compliance and Enforcement

8.1 Compliance Requirements

Compliance with this policy is mandatory for all personnel within scope. Personnel are expected to familiarise themselves with policy requirements and seek clarification when needed. Ignorance of policy requirements is not an acceptable excuse for violations.

Compliance may be verified through technical monitoring, audits, management oversight, and investigation of reported concerns. Personnel shall cooperate fully with compliance verification activities.

Acknowledgment of this policy is required as a condition of access to organizational systems. Personnel who have not acknowledged the policy shall not be granted system access.

8.2 Violations and Consequences

Violations of this policy are treated seriously and may result in disciplinary action proportionate to the severity and circumstances of the violation. Potential consequences include:

- Verbal or written warnings for minor or first-time violations.
- Mandatory additional training or counselling.
- Temporary or permanent revocation of system access or specific privileges.
- Suspension or demotion.
- Termination of employment or contract.
- Civil legal action to recover damages.
- Criminal referral for illegal activities.

Factors considered in determining appropriate consequences include the severity of the violation, whether the violation was intentional or negligent, the user's training and awareness, the user's compliance history, and the actual or potential impact of the violation.

8.3 Reporting Violations

Personnel shall report suspected policy violations or security concerns promptly through appropriate channels including:

- Direct manager or supervisor.
- IT Service Desk or Information Security team.
- Human Resources.
- Anonymous reporting hotline (if available).

Reports may be made anonymously where permitted by local law and organizational policy. Retaliation against personnel who report violations in good faith is strictly prohibited and will itself be treated as a serious violation.

9. Policy Exceptions

9.1 Exception Process

Exceptions to this policy may be granted in limited circumstances where legitimate business needs require and where compensating controls adequately address the risks created by the exception. Exceptions are not granted for convenience or personal preference.

Exception requests shall be submitted through the Security Exception Process (PRC-003) and must document the specific policy requirement for which an exception is requested, the business justification explaining why the exception is necessary, the proposed duration of the exception, compensating controls that will mitigate the risks, and the individual or team requesting the exception.

9.2 Exception Approval

Exception approval authority is based on the risk level of the exception:

- Low-risk exceptions may be approved by the IT Manager or Information Security Manager.
- Medium-risk exceptions require approval from the CISO or delegate.
- High-risk exceptions require approval from the Security Steering Committee or executive leadership.

- All exceptions shall be documented, time-limited, and subject to periodic review. Exceptions do not create precedent and each request is evaluated on its own merits.

9.3 Exception Documentation

Approved exceptions shall be documented with the specific scope and boundaries of the exception, the compensating controls implemented, the expiration date, the approving authority, and any monitoring or review requirements.

Exceptions shall be tracked in the exception register and reviewed at least annually. Expired exceptions must be renewed through the standard process or the excepted activity must cease.

10. Document Control

10.1 Document Information

Document Title	Acceptable Use Policy
Document ID	POL-002
Version	1.0
Classification	Internal Use
Effective Date	[Effective Date]
Next Review Date	[Review Date - typically 12 months from effective date]
Document Owner	[CISO Name], Chief Information Security Officer
Approved By	[CEO Name], Chief Executive Officer

10.2 Revision History

Version	Date	Author	Description of Changes
0.1	[Date]	[Author]	Initial draft
0.2	[Date]	[Author]	Incorporated review feedback
1.0	[Date]	[Author]	Approved for release

10.3 Approval Signatures

Role	Name	Signature	Date
Chief Executive Officer	[CEO Name]		
Chief Information Security Officer	[CISO Name]		
Chief Information Officer	[CIO Name]		

Appendix A: Acceptable Use Acknowledgment Form

I acknowledge that I have received, read, and understand the [Organization Name] Acceptable Use Policy (POL-002). I understand that compliance with this policy is mandatory and is a condition of my access to organizational information systems and technology resources.

I understand and agree that:

- I will use organizational systems primarily for legitimate business purposes and in accordance with this policy.
- I will protect my credentials and not share them with others under any circumstances.
- I have no expectation of privacy when using organizational systems.
- The organization may monitor my use of its systems without prior notice.
- Violations of this policy may result in disciplinary action up to and including termination.
- I am responsible for all activities conducted under my user accounts.
- I will report suspected security incidents or policy violations promptly.
- I will complete required security awareness training.

Employee/Contractor Name:	
Employee ID:	
Department:	
Signature:	
Date:	

Please return the signed acknowledgment form to Human Resources or the Information Security team. A copy will be retained in your personnel file.

Get the Complete Suite

This is just 1 of 120 documents in the Cybersecurity Governance Suite

ESSENTIALS SUITE

27 Documents | $149

21 Policies + 6 Essential Forms

STANDARD SUITE

82 Documents | $397

Policies + Standards + Processes + Procedures + Forms

ENTERPRISE SUITE

120 Documents | $697

Everything + AI Security Suite + GRC Add-Ons

Framework Aligned

NIST CSF 2.0 • ISO 27001:2022 • CIS Controls v8

Available on Gumroad and Payhip

Search: RidgeLine Cyber Defence