BASESECURE SAMPLE - EVALUATION ONLY

BASESECURE

SECURITY · POLICY · COMPLIANCE

Information Security Policy

Prepared for [COMPANY NAME]

Document Owner	[NAME / ROLE]
Approved By	[NAME / ROLE]
Effective Date	[DATE]
Next Review	[DATE]
Version	1.0
Classification	Internal Use Only

SAMPLE - NOT LICENSED FOR OPERATIONAL USE

BASESECURE SAMPLE - EVALUATION ONLY

Document Control

Version	Date	Author	Approved By	Summary of Changes
1.0	[DATE]	[NAME]	[NAME]	Initial release

1. Purpose

This policy establishes how [COMPANY NAME] protects the confidentiality, integrity, and availability of the information it creates, receives, stores, and transmits — including information belonging to its customers, employees, and business partners.

It is the master information security policy for the organization. All other security policies, standards, and procedures operate under it and must not conflict with it.

The objectives of this policy are to:

- Protect information assets against unauthorized access, disclosure, alteration, loss, and destruction.
- Ensure that security responsibilities are clearly assigned and understood.
- Meet applicable legal, regulatory, and contractual obligations.
- Enable the business to operate and grow without avoidable security disruption.
- Establish a consistent, documented basis for identifying and managing information security risk.

2. Scope

This policy applies to all employees, officers, contractors, temporary staff, interns, volunteers, and third-party users who access, process, store, or transmit [COMPANY NAME] information or use [COMPANY NAME] information systems — regardless of location, employment status, or device ownership.

It covers all information in any form, including electronic files, databases, email, printed material, and verbal communication, and all systems used to handle that information, including servers, workstations, mobile devices, network equipment, cloud services, and third-party platforms.

[Add or remove locations, subsidiaries, or systems as needed to reflect your actual environment.]

BASESECURE SAMPLE - EVALUATION ONLY

3. Roles and Responsibilities

Role	Responsibility
Executive Management	Approves this policy, sets risk tolerance, and provides the budget and authority needed to implement it.
[SECURITY LEAD]	Owns and maintains this policy, coordinates risk assessments, monitors compliance, and reports security matters to management.
[IT MANAGER / MSP]	Implements and operates technical controls, including access management, patching, backup, logging, and endpoint protection.
Human Resources	Ensures background screening, confidentiality agreements, security training, and timely onboarding and offboarding.
Managers and Supervisors	Ensure their teams complete required training, hold appropriate access only, and follow this policy day to day.
Data Owners	Classify the information under their control and approve who may access it.
All Personnel	Comply with this policy, protect credentials and information in their care, and promptly report suspected security incidents.
Third Parties	Meet the security obligations set out in their contract and in the Vendor and Third-Party Risk Policy.

4. Policy Requirements

[COMPANY NAME] applies the following requirements across its operations. Where a topic is governed by a supporting policy, that policy provides the detailed rules.

4.1 Security Governance

- Management formally approves this policy and reviews it at least annually.
- A named individual is accountable for information security at all times.
- Security policies are documented, published where all personnel can access them, and acknowledged by each person on hire and after any material revision.

4.2 Risk Management

- A documented information security risk assessment is performed at least annually and whenever a significant change occurs in the business, its technology, or its regulatory obligations.
- Identified risks are recorded in a risk register with an assigned owner, treatment decision, and target date.

BASESECURE SAMPLE - EVALUATION ONLY

- Risks accepted rather than remediated are approved in writing by [APPROVER ROLE] and reviewed at least annually.

4.3 Asset Management

- An inventory of hardware, software, cloud services, and data repositories is maintained and reviewed at least [FREQUENCY].
- Every asset has an assigned owner responsible for its protection and appropriate use.
- Assets are returned or securely wiped when personnel leave or when equipment is retired, and disposal is recorded.

4.4 Access Control

- Access is granted on the principles of least privilege and need to know, and is approved by the relevant data owner or manager before it is issued.
- Each user has a unique account. Shared or generic accounts are prohibited except where technically unavoidable, in which case use is approved, documented, and monitored.
- Multi-factor authentication is required for remote access, administrative accounts, email, and all externally accessible systems.
- Administrative privileges are limited to personnel who require them, are used only for administrative work, and are reviewed at least [FREQUENCY].
- User access rights are reviewed at least [FREQUENCY] and revoked immediately on termination or role change.

4.5 Data Classification and Handling

- Information is classified according to the Data Classification and Handling Policy, and handled according to its classification throughout its lifecycle.
- Confidential and regulated information is encrypted in transit and at rest.
- Information is retained only as long as required by business need, contract, or law, and is then securely destroyed.

4.6 Personnel Security

- Background screening is performed where permitted by law and proportionate to the role.
- All personnel sign a confidentiality or non-disclosure agreement before being granted access.
- Security awareness training is completed on hire and at least annually thereafter, and completion is recorded.
- Onboarding and offboarding follow documented checklists covering account creation, access revocation, and asset return.

BASESECURE SAMPLE - EVALUATION ONLY

4.7 Physical and Environmental Security

- Areas containing information systems or sensitive records are physically secured, and access is restricted to authorized personnel.
- Visitors to restricted areas are signed in and escorted.
- Workstations are locked when unattended, and sensitive material is not left exposed on desks, printers, or screens.

4.8 Operations Security

- Endpoint protection is deployed on all supported devices and kept current.
- Security patches are applied within [NUMBER] days for critical vulnerabilities and [NUMBER] days for all others; exceptions follow the process in section 6.
- Backups are performed [FREQUENCY], stored separately from production, protected against alteration, and restore-tested at least [FREQUENCY].
- Security-relevant events are logged, protected from tampering, retained for at least [DURATION], and reviewed for anomalies.
- Only software approved by [IT MANAGER / MSP] may be installed on company systems.

4.9 Network and Communications Security

- Networks are segmented so that a compromise in one area does not automatically expose others.
- Firewall and remote access rules are documented, justified, and reviewed at least [FREQUENCY].
- Remote access to internal systems is permitted only over an approved encrypted connection with multi-factor authentication.
- Wireless networks use current encryption standards, and guest wireless is isolated from the corporate network.

4.10 Change and Configuration Management

- Changes to production systems are requested, assessed for security impact, approved, and recorded before implementation.
- Systems are configured to a documented secure baseline; default credentials are changed and unnecessary services disabled before deployment.
- Emergency changes may be implemented immediately but must be documented and reviewed within [NUMBER] business days.

4.11 Third-Party and Vendor Security

- Vendors with access to [COMPANY NAME] information or systems are assessed for security risk before engagement and periodically thereafter.

BASESECURE SAMPLE - EVALUATION ONLY

- Contracts with such vendors include confidentiality, security, and breach notification obligations.
- Vendor access is limited to what the engagement requires and is revoked when the engagement ends.

4.12 Incident Management

- All personnel must report suspected security incidents to [REPORTING CONTACT] immediately and without fear of blame for good-faith reports.
- Incidents are triaged, contained, investigated, and resolved in accordance with the Incident Response Plan.
- Incidents are recorded, and those meeting defined thresholds are escalated to management, affected customers, regulators, or law enforcement within the timeframes required by contract and applicable law.
- A post-incident review is conducted for significant incidents, and resulting actions are tracked to completion.

4.13 Business Continuity

- Systems and processes critical to the business are identified, with defined recovery time and recovery point objectives.
- Continuity and recovery plans are documented and tested at least [FREQUENCY], and test results are recorded.

4.14 Compliance

- Legal, regulatory, and contractual security obligations applicable to [COMPANY NAME] are identified and tracked.
- Compliance with this policy is reviewed at least [FREQUENCY], and deficiencies are recorded and remediated.
- Personnel cooperate fully with authorized internal and external audits.

5. Related Documents

This policy is supported by, and read together with, the following documents:

- Acceptable Use Policy
- Access Control and Password Policy
- Data Classification and Handling Policy
- Incident Response Plan
- Backup and Disaster Recovery Plan

SAMPLE - NOT LICENSED FOR OPERATIONAL USE

BASESECURE SAMPLE - EVALUATION ONLY

- Vendor and Third-Party Risk Policy
- Remote Work Policy
- Mobile Device (BYOD) Policy
- Data Retention and Disposal Policy
- Employee Onboarding and Offboarding Security Checklists

[Remove any document your organization has not adopted. Do not reference a policy that does not exist — auditors check.]

6. Exceptions

Any exception to this policy must be requested in writing, include a business justification, an assessment of the resulting risk, and any compensating controls, and be approved by [APPROVER ROLE]. Approved exceptions are recorded in the exception register, given an expiry date, and reviewed at least annually.

7. Enforcement

Compliance with this policy is mandatory. Violations may result in disciplinary action up to and including termination of employment or contract, and may result in civil or criminal liability where applicable law provides for it. Third-party violations may result in suspension or termination of the engagement.

8. Review

This policy is reviewed by [SECURITY LEAD] at least annually, and additionally whenever a significant change occurs in the organization, its technology, its threat environment, or its legal and regulatory obligations. Material revisions require re-approval by management and re-acknowledgement by personnel.

9. Definitions

Term	Meaning
Information Asset	Any data, system, device, or service that holds value to the organization and requires protection.
Confidentiality	Ensuring information is accessible only to those authorized to have access.
Integrity	Ensuring information and processing methods remain accurate and complete.

BASESECURE SAMPLE - EVALUATION ONLY

Term	Meaning
Availability	Ensuring authorized users have access to information and systems when required.
Least Privilege	Granting each user only the access strictly necessary to perform their role.
Security Incident	Any event that compromises, or may compromise, the confidentiality, integrity, or availability of information or systems.
Third Party	Any external organization or individual engaged to provide goods or services.

10. Acknowledgement

I confirm that I have read and understood the [COMPANY NAME] Information Security Policy, and I agree to comply with it. I understand that failure to do so may result in disciplinary action.

Printed Name

Signature

Date

SAMPLE - NOT LICENSED FOR OPERATIONAL USE

BASESECURE SAMPLE - EVALUATION ONLY

Important Notice

> This document is a template. It must be reviewed and customized to reflect the actual operations, jurisdiction, contractual obligations, and risk profile of the organization using it.
>
> It does not constitute legal, regulatory, or compliance advice. It does not guarantee compliance with any framework, standard, regulation, or audit, and it does not guarantee certification of any kind.
>
> Consult qualified legal counsel and a licensed assessor before relying on this document to satisfy a regulatory or contractual obligation.

Licensed to a single organization unless a reseller or MSP license has been purchased. Redistribution or resale of this template is not permitted.

SAMPLE - NOT LICENSED FOR OPERATIONAL USE