[COMPANY NAME]
[Add your company logo / letterhead and registered address here]

Information Security Policy

HOW TO USE THIS TEMPLATE
This template is mostly complete and pre-filled with standard Indian practice. You should not have to fill many blanks.
Text in blue is a default that companies commonly change. Skim the blue text and edit only what differs for you.
Add your company name and letterhead once, in the header above. The body refers to "the Company".
This is the master Information Security Policy that sits above all the technical sub-policies (Acceptable Use, Access Control, Data Protection, Incident Response and so on). Name your security owner in Section 4, list the sub-policies you actually maintain in Section 8, and have the policy formally approved by management before you circulate it.
Have it reviewed by a qualified HR or legal professional before you adopt it, and delete this box.
Provided by CFOmatrix (cfomatrix.in). General template, not legal advice.

Policy owner	**[Human Resources / IT / Compliance]**
Effective date	**[DD MMM YYYY]**
Version	1.0
Approved by	**[Name, Title]**

1. Purpose

The Company depends on information and the systems that process it to run its business, serve its customers and meet its legal and contractual commitments. Information, in any form (electronic, paper, spoken or held by third parties), is a critical asset and must be protected against loss, misuse, unauthorised access and disclosure.

This Information Security Policy (the "Policy" or "ISP") is the master, top level policy of the Company's information security management system. It sets out the Company's objectives, governance, roles, risk based approach and overarching rules for protecting information, and it provides the umbrella under which all subordinate security policies, standards and procedures operate.

The objectives of this Policy are to preserve the three core properties of information security, the "CIA triad":

- Confidentiality: ensuring that information is accessible only to those authorised to have access, and protected against unauthorised disclosure.
- Integrity: safeguarding the accuracy, completeness and reliability of information and processing methods, and preventing unauthorised or undetected modification.
- Availability: ensuring that authorised users have reliable and timely access to information and systems when required.

In support of these properties, the Policy also seeks to protect the authenticity, accountability, non-repudiation and resilience of information and systems, to comply with applicable law and contractual obligations, and to build a culture of security awareness across the workforce.

2. Scope

This Policy applies across the whole of the Company and is binding on:

- All employees, whether permanent, temporary, probationary, trainee or part time.
- Directors, officers and members of senior management.
- Contractors, consultants, interns, secondees, temporary staff and any agency or vendor personnel who access Company information or systems.
- Third parties, including service providers, processors and partners, to the extent set out in their contracts.

The Policy covers all information assets owned, controlled or processed by the Company, regardless of form or location, including:

- Data and information in electronic, printed, spoken, visual or any other form.
- All information systems, applications, databases, source code and platforms, whether on premises, hosted, cloud based or **SaaS**.
- All computing and network infrastructure, including servers, endpoints, laptops, mobile devices, networking equipment, storage and backup media.
- Company owned, Company managed and personal devices used to access Company information under any **Bring Your Own Device (BYOD)** arrangement.
- All locations from which Company information is accessed, including offices, **remote and work from home** locations, client sites and while travelling.

No system, location or category of user is out of scope. Where a specific exception is required, it must follow the exceptions process in Section 11.

3. Definitions

- "Information asset": any data, system, device, service or document that has value to the Company and warrants protection.
- "Information owner" (asset owner): the manager or function accountable for a given information asset, its classification and the decisions about who may access it.
- "Custodian": the person or team responsible for the day to day operation, maintenance and technical protection of an asset on the owner's behalf.
- "User": any individual who is granted access to Company information or systems.
- "Personal data" and "data principal": as defined under the Digital Personal Data Protection Act, 2023 (the "DPDP Act"); personal data is any data about an identifiable individual, and a data principal is the individual to whom it relates.

- "Security incident": any actual or suspected event that compromises, or could compromise, the confidentiality, integrity or availability of information or systems.
- "Confidential information": any non public information of the Company, its customers, employees or partners, including the classification levels defined in Section 7.

4. Governance, Roles and Responsibilities

Information security is a shared responsibility. The Company adopts a clear governance structure so that accountability is never ambiguous.

4.1 Management and the Board

Senior management owns information security at the Company. Management approves this Policy, sets the risk appetite, provides the budget and resources for security, and reviews the security posture at least **annually**. Management visibly champions security and holds the organisation accountable for compliance.

4.2 Security owner

The **CISO / Security Owner** (or, where no dedicated officer exists, the **Head of IT** acting as the designated security owner) has overall operational responsibility for the information security programme. This role:

- Maintains, communicates and enforces this Policy and the supporting sub-policies, standards and procedures.
- Owns the risk assessment process and the risk register, and proposes risk treatment.
- Coordinates security operations, monitoring, vulnerability management and incident response.
- Reports the security posture, key risks and incidents to management.
- Owns the awareness and training programme and the audit and compliance calendar.

4.3 Information Security governance forum

An **Information Security Steering Committee**, chaired by the security owner and including representatives from **IT, HR, Legal/Compliance and key business functions**, meets at least **quarterly** to review risks, incidents, policy exceptions, audit findings and the improvement roadmap.

4.4 Other roles

Role	Key responsibilities
Information / asset owners	Classify assets, authorise access, review access **half yearly**, approve exceptions for their assets
IT / Operations	Implement and maintain technical controls, patching, backups, logging and hardening

Data Protection Officer / **privacy contact**	Oversee DPDP Act compliance, handle data principal requests and grievances
Human Resources	Pre employment screening, onboarding/offboarding access changes, disciplinary action
Legal / Compliance	Advise on legal and contractual obligations, regulatory reporting, contracts with processors
Managers	Ensure their teams complete training, follow this Policy and report incidents promptly
All users	Protect assets in their care, follow the Policy, report incidents and suspected breaches

5. Risk Based Approach

The Company manages information security through a continuous, risk based process rather than as a one time exercise. The approach is consistent with the ISO/IEC 27001 information security management system model and the SOC 2 Trust Services Criteria.

- Asset and risk identification: the Company maintains an inventory of information assets and conducts a documented risk assessment at least **annually** and whenever there is a significant change (new system, major incident, new business line or material change in the threat landscape).
- Risk evaluation: risks are assessed by likelihood and impact and recorded in a risk register with an assigned owner.
- Risk treatment: for each significant risk the Company selects a treatment, namely mitigate (apply controls), transfer (for example insurance or contractual allocation), avoid (stop the activity) or accept (with documented, time bound sign off by an appropriate authority).
- Controls: controls are selected to bring residual risk within the Company's risk appetite and are mapped to recognised frameworks (see Section 8 and Section 13). Residual risk above the agreed threshold must be accepted in writing by **senior management**.
- Monitoring and review: the effectiveness of controls is monitored on an ongoing basis, with the risk register reviewed at least **quarterly** by the governance forum.

6. Core Security Principles and Control Areas

All Company systems and behaviours must uphold the following principles, which are detailed in the supporting sub-policies referenced in Section 8.

- Least privilege and need to know: users and systems are granted only the minimum access required for their role, for the minimum time necessary.
- Defence in depth: security relies on multiple layers of control rather than any single safeguard.
- Secure by design and by default: security and privacy are built into systems, projects and changes from the start, not added afterwards.

- Segregation of duties: critical tasks are split so that no single individual can complete a sensitive action unchecked.
- Identity and access management: access is uniquely identifiable, authenticated, authorised and logged. Multi factor authentication is required for **remote access, administrative accounts and all internet facing systems**. Access is reviewed at least **every six months** and revoked promptly on role change or exit.
- Endpoint and network security: endpoints must run approved anti malware, full disk encryption and current patches; networks are segmented, firewalled and monitored.
- Cryptography: data in transit must use **TLS 1.2 or higher** and sensitive data at rest must be encrypted using **AES-256** or equivalent; keys are managed securely.
- Secure development: code is developed, reviewed and tested securely, with secrets kept out of source code and vulnerabilities remediated within defined timelines.
- Logging and monitoring: security relevant events are logged, protected from tampering, retained for at least **180 days** and monitored for anomalies.
- Backup and resilience: critical data is backed up per the **3-2-1** principle, backups are tested at least **quarterly**, and business continuity and disaster recovery plans are maintained and exercised.
- Physical security: server rooms, network equipment and sensitive areas are physically secured with controlled and logged access.
- Vulnerability and patch management: vulnerabilities are scanned regularly; critical patches are applied within **15 days** of release, high within **30 days**.
- Vendor and third party security: third parties with access to Company information are assessed, contractually bound to equivalent controls and reviewed periodically.

7. Information Classification and Handling

All information must be classified by its owner so that the right level of protection is applied. The Company uses the following standard scheme:

Classification	Description	Example	Minimum handling
Public	Approved for release to anyone	Marketing material, published website	No restriction once approved for release
Internal	For internal use; not for public release	Internal memos, org charts	Share only within the Company on a need to know basis
Confidential	Sensitive business or personal data	Customer data, financials, HR records, source code	Encrypt in transit and at rest; access on need to know; no unmanaged storage
Restricted / Highly Confidential	Most sensitive; serious harm if disclosed	Trade secrets, credentials, special category personal data	Strict least privilege, encryption, logging, explicit owner approval to share

Information must be labelled, stored, transmitted, shared and disposed of in line with its classification. Personal data is additionally governed by the Data Protection sub-policy and the DPDP Act (see Section 9). Media and documents must be securely wiped or destroyed at end of life.

8. Supporting Policies, Standards and Procedures

This master Policy is implemented through a set of subordinate documents. Each is owned by the security owner, approved by management and reviewed at least **annually**. The Company maintains the following sub-policies (adjust the list to those you actually operate):

- **Acceptable Use Policy** (use of systems, internet, email and devices).
- **Access Control and Identity Management Policy**.
- **Password and Authentication Standard**.
- **Data Protection and Privacy Policy** (DPDP Act compliance).
- **Data Classification and Handling Standard**.
- **Cryptography and Key Management Standard**.
- **Endpoint, Mobile and BYOD Security Policy**.
- **Network and Cloud Security Standard**.
- **Secure Software Development and Change Management Policy**.
- **Vulnerability and Patch Management Standard**.
- **Logging and Monitoring Standard**.
- **Backup, Business Continuity and Disaster Recovery Policy**.
- **Physical and Environmental Security Policy**.
- **Third Party / Vendor Risk Management Policy**.
- **Information Security Incident Response Plan**.
- **Acceptable Use of AI and Generative AI Tools Policy**.

Where any sub-policy conflicts with this master Policy, this master Policy prevails unless the sub-policy is more restrictive, in which case the more restrictive requirement applies.

9. Data Protection and Privacy

Where the Company processes personal data, it does so in accordance with the Digital Personal Data Protection Act, 2023 and the rules made under it (the DPDP framework is still being finalised and will be updated as it evolves). The Data Protection and Privacy sub-policy gives full effect to these obligations; the key requirements are:

- Lawful processing and consent: personal data is processed only for a lawful purpose, with the data principal's consent or another permitted legal basis, supported by a clear notice.
- Purpose and storage limitation: data is collected only for specified purposes, used only for those purposes, and retained no longer than necessary or as required by law.
- Data principal rights: the Company honours rights to access, correction, completion, updating, erasure and grievance redressal, and the right to nominate.

- Data processors: any processor engaged by the Company is bound by a written contract requiring equivalent protection and processing only on the Company's instructions.
- Breach notification: a personal data breach is reported to the Data Protection Board of India and to affected data principals as required under the DPDP framework, in addition to the incident process in Section 10.
- Grievance and contact: data principals may contact the **Data Protection Officer / privacy contact** at **privacy@company.com** for grievances and requests.

10. Security Incident Management and Reporting

Every user must report any actual or suspected security incident, data breach, lost or stolen device, phishing attempt or policy violation immediately, and no later than **1 hour** of becoming aware, to **security@company.com** or the **IT helpdesk**. Users must not attempt to investigate or remediate on their own beyond making the situation safe.

The Company maintains a documented Incident Response Plan covering detection, triage, containment, eradication, recovery, evidence preservation and post incident review. Statutory and regulatory reporting timelines must be met, including:

- CERT-In: cyber incidents of the type specified in the CERT-In Directions, 2022 must be reported to CERT-In within 6 hours of detection or notification.
- DPDP Act: personal data breaches must be notified to the Data Protection Board of India and affected data principals as required (see Section 9).
- Contractual: customer and partner notification obligations in contracts must be honoured within their stated timelines.

A post incident review with root cause analysis and corrective actions is conducted for every significant incident, and lessons learned feed back into the risk register and controls.

11. Exceptions

From time to time a business need may require a deviation from this Policy or a sub-policy. Exceptions must follow a formal, documented process:

- The requester submits an exception request describing the requirement, the control affected, the duration sought and the business justification.
- The risk is assessed by the **CISO / Security Owner**, with compensating controls identified.
- The exception is approved in writing by the **CISO / Security Owner** and, for high risk exceptions, by **senior management**.
- Every exception is time bound (maximum **6 months**), recorded in an exceptions register, and reviewed at expiry. No exception is open ended.

Undocumented deviations are violations of this Policy and are not permitted.

12. Compliance, Enforcement and Consequences

Compliance with this Policy is mandatory. The Company verifies compliance through monitoring, internal and external audits, vulnerability assessments, **penetration tests** and management reviews. Users are required to acknowledge this Policy on joining and on each **annual** update, and to complete security awareness training at induction and at least **annually** thereafter.

Information and systems may be monitored and logged for security and compliance purposes, to the extent permitted by law and subject to applicable privacy obligations. Users should have no expectation of privacy in their use of Company systems beyond what the law requires.

Violation of this Policy may result in disciplinary action up to and including termination of employment or engagement, in accordance with the Company's disciplinary process, and may also lead to civil or criminal liability where the conduct breaches applicable law (including the Information Technology Act, 2000, the DPDP Act, 2023, and, for bribery or corruption involving systems or data, the Prevention of Corruption Act, 1988, and the FCPA or UK Bribery Act for cross border dealings). Contractors and vendors who breach the Policy may have their contracts terminated.

13. Legal, Regulatory and Contractual Compliance

This Policy is designed to help the Company meet its legal, regulatory and contractual obligations, including but not limited to:

- The Information Technology Act, 2000 and rules made under it.
- The Digital Personal Data Protection Act, 2023 (DPDP framework, evolving).
- The CERT-In Directions, 2022 on incident reporting and related cyber hygiene requirements.
- Sector and customer specific contractual security requirements, including obligations under **customer Data Processing Agreements**.

The Company aligns its control framework with the recognised standards **ISO/IEC 27001** and the **SOC 2** Trust Services Criteria (Security, and where applicable Availability, Confidentiality, Processing Integrity and Privacy), to provide assurance to customers and partners. Mapping of internal controls to these frameworks is maintained by the security owner.

14. Review and Governance

This Policy is owned by the **CISO / Security Owner** and approved by **senior management**. It is reviewed at least **once every 12 months** and additionally whenever there is a material change in the business, technology, threat landscape, applicable law or following a significant security incident.

Proposed changes are reviewed by the **Information Security Steering Committee** and approved by management before publication. The current approved version supersedes all previous versions. Records of versions, approvals and review dates are maintained as shown below.

Field	Value

[COMPANY NAME]

[Add your company logo / letterhead and registered address here]

Policy owner	**CISO / Security Owner**
Approved by	**Senior Management / Board**
Version	**1.0**
Effective date	**DD-MMM-YYYY**
Next review date	**DD-MMM-YYYY**