## **INFORMATION SECURITY POLICY TEMPLATE**

##

##

## **[Company Name][Address] [Contact]**

**Document Control**

Document Reference: ISP-[Unique ID or Code]

Version: [Version Number]

Effective Date: [DD/MM/YYYY]

Last Reviewed: [DD/MM/YYYY]

Next Review Date: [DD/MM/YYYY]

Prepared By: [Document Owner / Author Name or Role]

Approved By: [Approver Name / Position]

Confidentiality Level: [Public / Internal Use / Confidential]

##

##

[**INFORMATION SECURITY POLICY TEMPLATE**](#_wwnx4d5ncvnh) **4**

[**1. Policy Statement**](#_mut2f8yrzriu) **4**

[**2. Purpose of the Policy**](#_qc94wj36512n) **4**

[**3. Scope**](#_tmx8y64jp5b0) **4**

[**4. Definitions**](#_mkseqvqzqwqp) **4**

[**5. Roles and Responsibilities**](#_il76sduqpjg) **5**

[Executive Management](#_cjwbeyp5fc79) 5

[Information Security Officer (ISO)](#_qf6kyp3bubrp) 5

[Department Heads](#_em3nlctk63kx) 5

[All Employees](#_5c05m27k02j3) 5

[**6. Information Classification**](#_wi4rw3pz5wwu) **6**

[Data Categories](#_sdm1651dp6se) 6

[Handling of Sensitive Data](#_j6dizicrq4t7) 6

[**7. Acceptable Use Policy (AUP)**](#_x8lo2b3hmxmx) **7**

[Device Usage](#_c19tu87j0q66) 7

[Internet & Email Usage](#_xhisdbcmilc) 7

[Remote Work Guidelines](#_tgfxb6opdyaz) 7

[**8. Access Control**](#_bc9aznqsvlp9) **8**

[User Access Management](#_dxs2ys5la2uy) 8

[Password Requirements & Multi-Factor Authentication (MFA)](#_n5z0uyyoujur) 8

[Privileged Access Control](#_9dqeb3b5jjpt) 8

[**9. Data Protection & Privacy**](#_vebry32brawt) **8**

[Data Storage & Backup](#_1rs4r22iplbz) 9

[Data Transmission Security](#_nxcawygfj1mh) 9

[Data Retention & Disposal Guidelines](#_h2ws412w87c8) 9

[**10. Physical Security Measures**](#_x3einiogn4j9) **9**

[Office Access](#_6d10n7jdxv7u) 9

[Securing Devices and Assets](#_amt2qiq6id5z) 10

[**11. Network Security Controls**](#_utf5r627kca5) **10**

[Firewall & Network Segmentation](#_tb83qq1nzx38) 10

[Secure Wi-Fi Practices](#_1rm3vnyq6jqn) 10

[**12. Incident Reporting and Response**](#_45yfos1eqwhy) **10**

[Incident Detection](#_jqgk8a3at4en) 11

[Reporting Workflow](#_3gnptdujzrnz) 11

[Response Team Responsibilities](#_qdz05mve5ggs) 11

[**13. Monitoring and Auditing**](#_rwrkzeia8eug) **12**

[System & Network Monitoring](#_qlq4ud5r9ina) 12

[Audit Log Retention](#_49sft1503e45) 12

[**14. Third-Party and Vendor Security**](#_ubhylm2yk7vs) **12**

[Vendor Risk Management](#_wuil774842hh) 12

[Third-Party Access Guidelines](#_nsyzl51it3nx) 13

[**15. Training and Awareness**](#_tl4t3n7ebppg) **13**

[Security Training Programs](#_9gbhhwim8cqm) 13

[Employee Acknowledgments](#_250qwtlatehl) 13

[**16. Policy Compliance and Enforcement**](#_slrwg4cfz9jz) **13**

[Compliance Monitoring](#_y2176aywi38p) 14

[Disciplinary Actions for Non-Compliance](#_rsvzvuajdlm) 14

[**17. Policy Review and Updates**](#_pnej4ckd7srz) **14**

[Review Schedule (Annually, As Needed)](#_j4l0szmz9plf) 14

[Amendment Process](#_z3de74z7898p) 14

##

## **INFORMATION SECURITY POLICY TEMPLATE**

## **1. Policy Statement**

[Company Name] is committed to safeguarding the confidentiality, integrity, and availability of its information assets. This Information Security Policy serves as a formal declaration of our dedication to maintaining a secure information environment that supports business operations, protects client trust, and ensures compliance with applicable legal, regulatory, and contractual obligations. All employees, contractors, and partners are expected to uphold the principles outlined in this policy, fostering a culture of security awareness across the organization.

## **2. Purpose of the Policy**

The purpose of this policy is to establish a structured framework for managing information security within [Company Name]. It provides clear guidelines on protecting sensitive information from unauthorized access, misuse, disclosure, alteration, and destruction. This policy ensures that information security is integrated into every business process, aligning with best practices, industry standards, and regulatory requirements. It is designed to minimize risks, reduce vulnerabilities, and ensure that information assets are managed responsibly throughout their lifecycle.

## **3. Scope**

This policy applies to all employees, contractors, consultants, interns, and third-party vendors who have access to [Company Name]’s information systems, data, and physical assets. It encompasses all forms of information—electronic, printed, verbal, and visual—and extends to all computing devices, network infrastructure, cloud services, and physical facilities managed or operated by [Company Name]. The scope of this policy includes, but is not limited to, data processing systems, communication networks, software applications, and personal devices used for business purposes under a Bring Your Own Device (BYOD) policy.

## **4. Definitions**

For clarity and consistent understanding, the following key terms are defined as they apply to this policy:

* **Information Assets**: Any data, system, hardware, software, or resource that holds value to [Company Name] and requires protection.
* **Confidential Information**: Sensitive business or personal data that, if disclosed or accessed improperly, could harm [Company Name] or its clients.
* **Information Security Officer (ISO)**: The designated individual responsible for overseeing the implementation and monitoring of information security practices.
* **Access Control**: Procedures and technologies used to restrict access to information systems and data based on user roles and authorization levels.
* **Security Incident**: Any event that compromises the confidentiality, integrity, or availability of information assets, including data breaches, system intrusions, and unauthorized disclosures.

## **5. Roles and Responsibilities**

Information security is a shared responsibility that requires coordinated efforts across all levels of the organization. The following roles are accountable for enforcing and maintaining the standards set forth in this policy:

### **Executive Management**

Executive Management holds the ultimate responsibility for the organization’s information security posture. They provide strategic direction, allocate necessary resources, and ensure that security initiatives align with business objectives. Management is also accountable for endorsing the policy and setting the tone for a security-conscious culture.

### **Information Security Officer (ISO)**

The ISO is responsible for the development, implementation, and oversight of the organization’s information security program. This role involves monitoring compliance with the policy, managing risk assessments, coordinating incident response activities, and ensuring that security controls are effective and up-to-date. The ISO also serves as the primary point of contact for internal and external security audits.

### **Department Heads**

Department Heads are responsible for ensuring that their teams understand and adhere to the Information Security Policy. They must communicate security expectations, facilitate necessary training, and report any security incidents or policy violations to the ISO. Department Heads also play a crucial role in ensuring that security measures are effectively integrated into departmental workflows.

### **All Employees**

Every employee is expected to follow the information security guidelines set forth in this policy. This includes protecting company information, using systems responsibly, attending mandatory security training, and reporting any suspected security incidents or vulnerabilities to the appropriate personnel. Employees are accountable for maintaining the confidentiality of information they handle and for adhering to acceptable use standards for all company resources.

## **6. Information Classification**

[Company Name] shall classify all information assets based on their sensitivity, value, and criticality to business operations. Information classification ensures that data is handled, stored, and transmitted in a manner appropriate to its level of confidentiality and risk. All employees and third parties with access to [Company Name]’s information are required to adhere to these classification guidelines.

### **Data Categories**

All information assets shall be categorized into one of the following classifications:

* **Public**: Information intended for public disclosure. Unauthorized access or distribution poses no risk to [Company Name]. Examples include marketing materials, publicly available reports, and press releases.
* **Internal Use Only**: Information meant for use within the organization. Unauthorized disclosure may cause minor operational inconvenience but not significant damage. Examples include internal procedures, project documents, and internal communications.
* **Confidential**: Sensitive information that, if disclosed to unauthorized parties, could cause harm to [Company Name], its clients, or partners. This includes client data, financial records, proprietary business information, and personal data protected under privacy regulations.

### **Handling of Sensitive Data**

All employees and contractors must handle confidential and sensitive information with the highest level of care. Confidential data must be accessed only by authorized personnel, stored securely with encryption where applicable, and transmitted using secure communication channels. Physical copies of sensitive information should be stored in locked cabinets and disposed of through secure shredding when no longer required.

Information classified as Confidential must not be shared externally without proper authorization. Any suspected compromise or mishandling of sensitive data must be reported immediately to the Information Security Officer for investigation and remediation.

## **7. Acceptable Use Policy (AUP)**

All employees, contractors, and third-party users are required to use [Company Name]’s information systems, devices, and network resources responsibly and in accordance with this Acceptable Use Policy. The purpose of these guidelines is to protect the integrity, availability, and security of company assets while enabling productive and secure business operations.

### **Device Usage**

All computing devices, whether company-owned or approved personal devices, must be used in a manner that supports business objectives and adheres to security protocols. Users are responsible for ensuring that devices used for business purposes are secured with up-to-date antivirus software, device encryption, and strong access controls. Unauthorized installation of software, tampering with security settings, or using devices for activities that violate company policies is strictly prohibited.

### **Internet & Email Usage**

Internet access and email services provided by [Company Name] are intended for business-related activities. Limited personal use is permitted, provided it does not interfere with work duties, consume excessive resources, or violate any laws or company policies. The following activities are expressly prohibited:

* Accessing or distributing offensive, illegal, or inappropriate content.
* Using company email for unauthorized personal gain or unsolicited commercial messaging (spam).
* Downloading or sharing files that could introduce security risks to the organization’s network.
 All email communications must reflect professionalism and comply with data protection and confidentiality standards.

### **Remote Work Guidelines**

Employees working remotely must ensure that their work environment supports the secure handling of company information. Access to corporate systems must be conducted through secure VPN connections, and remote devices must comply with company security configurations, including up-to-date software patches and multi-factor authentication (MFA). Sensitive information should not be discussed in public spaces, and physical documents must be stored securely, even when off-site. Any loss or theft of remote devices must be reported immediately to the Information Security Officer.

## **8. Access Control**

[Company Name] enforces strict access control measures to ensure that only authorized individuals have access to information systems, data, and resources necessary for their job functions. Access rights are granted based on the principle of least privilege and are reviewed regularly to prevent unauthorized access, data breaches, and misuse of information assets.

### **User Access Management**

User access to information systems shall be provisioned based on defined roles and responsibilities. Access requests must follow a formal approval process, with appropriate authorization from department heads or the Information Security Officer. All user accounts must be unique to ensure accountability and traceability of activities. Access privileges must be promptly revoked upon employee termination or change in job roles. Periodic reviews of user access rights will be conducted to ensure continued relevance and compliance.

### **Password Requirements & Multi-Factor Authentication (MFA)**

All users are required to adhere to [Company Name]’s password standards to prevent unauthorized access to systems and data. Passwords must meet complexity requirements, including a minimum length, the use of uppercase and lowercase letters, numbers, and special characters. Passwords must be changed regularly and must not be shared or reused across different systems.

Wherever feasible, Multi-Factor Authentication (MFA) shall be implemented to provide an additional layer of security, especially for accessing critical systems, remote access solutions, and privileged accounts. MFA enhances security by requiring users to verify their identity through an additional method, such as a mobile authenticator or biometric verification.

### **Privileged Access Control**

Access to administrative and privileged accounts shall be strictly controlled and limited to personnel who require elevated permissions to perform their job duties. The use of privileged accounts must be monitored and logged to detect any unauthorized activities. Privileged account credentials must be stored securely and rotated regularly to mitigate risks associated with credential theft or misuse. Any temporary elevation of access rights for specific tasks must be documented and revoked immediately after task completion.

## **9. Data Protection & Privacy**

[Company Name] is committed to protecting the privacy of personal and sensitive information in accordance with applicable data protection laws and industry best practices. All data must be handled with care, ensuring it is stored, transmitted, and disposed of securely to prevent unauthorized access, loss, or misuse. Employees are required to follow the guidelines outlined in this policy when processing or managing any form of company data.

### **Data Storage & Backup**

All critical business data must be stored in secure, authorized storage solutions managed by [Company Name]. Data residing on end-user devices must be minimized, and where necessary, must be encrypted to prevent unauthorized access. Regular data backups shall be performed to ensure business continuity and protect against data loss. Backup data must be stored securely, with access restricted to authorized personnel only. The integrity and availability of backups will be tested periodically to ensure effectiveness.

### **Data Transmission Security**

All data transmitted over public or unsecured networks must be encrypted using secure communication protocols such as HTTPS, SFTP, or VPNs. Sensitive information, including personal data and confidential business information, must not be transmitted via unencrypted email or unsecured channels. Employees must ensure that data shared with external parties is done through approved, secure methods that comply with [Company Name]’s data handling standards.

### **Data Retention & Disposal Guidelines**

Data must be retained only for as long as necessary to fulfill its intended business purpose or to meet legal and regulatory obligations. [Company Name] will maintain a data retention schedule that specifies retention periods for various types of information. Upon reaching the end of the retention period, data must be securely disposed of in a manner that ensures it cannot be reconstructed or retrieved. Electronic data must be permanently deleted using secure erasure tools, while physical documents must be shredded or incinerated.

## **10. Physical Security Measures**

[Company Name] is committed to maintaining robust physical security controls to protect its facilities, information systems, and physical assets from unauthorized access, theft, or damage. All personnel must comply with the organization’s physical security procedures to ensure a secure working environment and safeguard sensitive information.

### **Office Access**

Access to [Company Name]’s office premises shall be restricted to authorized personnel only. Entry to secured areas, such as server rooms or storage facilities containing sensitive information, will be controlled through access cards, keycodes, or biometric systems. Visitors and contractors must be registered at reception, provided with visitor badges, and escorted by authorized staff at all times. Unauthorized individuals found in restricted areas will be reported immediately to security personnel or the Information Security Officer.

### **Securing Devices and Assets**

All company-issued laptops, mobile devices, and other portable equipment must be secured when not in use. Employees are responsible for safeguarding their devices both on-site and while working remotely. Workstations must be locked when unattended, and portable devices must never be left in unsecured public locations. Sensitive physical documents must be stored in locked cabinets or drawers when not actively used and should not be left exposed on desks or shared workspaces. Asset inventories will be maintained and audited periodically to ensure accountability and control over company equipment.

## **11. Network Security Controls**

[Company Name] implements comprehensive network security measures to protect its IT infrastructure from unauthorized access, cyberattacks, and internal misuse. All network-related activities must comply with the security controls outlined in this policy to ensure the confidentiality, integrity, and availability of business-critical systems and data.

### **Firewall & Network Segmentation**

Firewalls shall be deployed at all network entry and exit points to monitor and control incoming and outgoing traffic based on predefined security rules. Firewalls will be configured to block unauthorized access attempts and protect against external threats. Internal network segmentation will be used to isolate sensitive systems, such as servers and databases, from general user networks. This segmentation reduces the risk of lateral movement within the network in the event of a security breach. Firewall configurations and segmentation rules will be reviewed periodically to ensure they remain effective and aligned with emerging threats.

### **Secure Wi-Fi Practices**

All wireless networks within [Company Name] facilities must be secured using strong encryption protocols, such as WPA3 or equivalent. Default router passwords must be changed, and Wi-Fi networks will employ hidden SSIDs to reduce visibility to unauthorized users. Guest Wi-Fi access will be provided through a separate, isolated network to prevent access to internal resources. Employees must not connect personal devices to internal business Wi-Fi without prior authorization and verification of device security compliance. Wireless networks will be monitored for unauthorized access attempts and rogue devices.

## **12. Incident Reporting and Response**

[Company Name] is committed to a structured and efficient approach for managing information security incidents to minimize impact and restore normal operations as quickly as possible. All employees, contractors, and third parties are required to report suspected or actual security incidents promptly, following the established procedures to ensure timely detection, containment, and resolution.

### **Incident Detection**

All users of [Company Name]’s information systems are responsible for remaining vigilant and reporting any unusual or suspicious activities that may indicate a security incident. Potential indicators include unauthorized access attempts, malware infections, data breaches, system performance anomalies, or any behavior that deviates from normal operational patterns. The IT department will utilize automated monitoring tools and intrusion detection systems (IDS) to proactively identify threats and vulnerabilities within the network.

### **Reporting Workflow**

All security incidents, regardless of severity, must be reported immediately to the Information Security Officer (ISO) or the designated incident response team. Reports can be submitted through official communication channels such as email, internal reporting portals, or phone hotlines. The incident report should include a description of the event, systems or data affected, and any immediate actions taken by the reporter. Upon receiving the report, the ISO will classify the incident, determine its impact, and initiate the appropriate response procedures.

### **Response Team Responsibilities**

The incident response team, led by the ISO, is responsible for coordinating all actions related to the containment, investigation, mitigation, and recovery of security incidents. Their responsibilities include:

* Assessing the scope and impact of the incident.
* Implementing containment measures to prevent further damage.
* Conducting a thorough investigation to determine root causes.
* Communicating with stakeholders, including management, legal teams, and external authorities if required.
* Overseeing the recovery process and restoring affected systems and services.
* Documenting the incident response process and conducting a post-incident review to identify lessons learned and recommend improvements to prevent future occurrences.

## **13. Monitoring and Auditing**

[Company Name] shall implement continuous monitoring and auditing practices to ensure the security and integrity of its information systems. These measures are essential for detecting unauthorized activities, verifying compliance with security policies, and supporting incident investigation and forensic analysis. All monitoring activities will be conducted in a manner that respects employee privacy while fulfilling security and compliance requirements.

### **System & Network Monitoring**

Information systems and network infrastructure will be continuously monitored using automated tools to detect anomalies, suspicious activities, and potential security incidents. Monitoring will include, but is not limited to, system access logs, network traffic patterns, user activities, and changes to critical configurations. Alerts generated by monitoring systems will be reviewed and investigated by the IT or security team in a timely manner. Regular security assessments and vulnerability scans will also be performed to identify and remediate potential weaknesses.

### **Audit Log Retention**

Audit logs capturing user activities, system events, access attempts, and security-related actions shall be maintained to support accountability and traceability. Logs must be protected against unauthorized access, alteration, or deletion, ensuring their integrity for audit and forensic purposes. [Company Name] will define and adhere to a log retention policy, ensuring that logs are retained for a minimum period as required by legal, regulatory, or contractual obligations, typically no less than 12 months. Archived logs will be stored securely and accessible only to authorized personnel for review and analysis.

## **14. Third-Party and Vendor Security**

[Company Name] recognizes that third-party service providers and vendors can introduce security risks if not properly managed. To protect information assets and maintain a secure operational environment, all third-party engagements must adhere to strict security requirements. This policy ensures that external partners handle [Company Name]’s data with the same level of care and protection as internal personnel.

### **Vendor Risk Management**

Before engaging with any third-party vendor, a comprehensive risk assessment must be conducted to evaluate their information security posture. Vendors must demonstrate compliance with relevant data protection regulations and industry best practices. Contracts and service level agreements (SLAs) will include specific clauses addressing information security requirements, confidentiality obligations, data handling procedures, and incident reporting expectations. Periodic audits or security assessments may be performed on critical vendors to ensure ongoing compliance and to address emerging risks throughout the business relationship.

### **Third-Party Access Guidelines**

Access to [Company Name]’s systems, networks, or data by third parties will be granted on a need-to-know basis and must follow the principle of least privilege. All third-party access must be authorized in advance by the Information Security Officer (ISO) and be time-bound to the duration necessary for task completion. Remote access will require the use of secure connections, such as VPNs, and may be subject to additional security controls like Multi-Factor Authentication (MFA). Vendor activities will be monitored and logged to ensure compliance with access restrictions, and any violation of access guidelines will result in immediate revocation of access and potential contractual penalties.

## **15. Training and Awareness**

[Company Name] is committed to fostering a culture of security awareness across the organization. To ensure that all employees understand their responsibilities in protecting information assets, mandatory security training and ongoing awareness initiatives will be provided. These programs are designed to equip personnel with the knowledge and skills necessary to recognize and respond to potential security threats effectively.

### **Security Training Programs**

All new employees must complete an information security orientation as part of their onboarding process. This initial training will cover key topics such as data protection practices, acceptable use policies, phishing awareness, password management, and incident reporting procedures. In addition to onboarding training, [Company Name] will conduct periodic refresher courses and targeted security awareness campaigns to address emerging threats and evolving compliance requirements. Specialized training sessions may be organized for specific roles that handle sensitive data or have elevated access privileges.

### **Employee Acknowledgments**

Employees are required to formally acknowledge their understanding and acceptance of [Company Name]’s Information Security Policy upon completion of training programs. Acknowledgment forms must be signed and retained in employee records as proof of compliance. These acknowledgments confirm the employee’s commitment to adhering to security guidelines and their awareness of the consequences of policy violations. Failure to complete mandatory training or acknowledgment processes may result in disciplinary actions in accordance with company procedures.

## **16. Policy Compliance and Enforcement**

Compliance with this Information Security Policy is mandatory for all employees, contractors, and third-party partners of [Company Name]. Adherence to the outlined security practices is essential to protect the organization’s information assets, maintain regulatory compliance, and uphold client trust. Failure to comply with this policy will result in enforcement actions as defined in this section.

### **Compliance Monitoring**

[Company Name] will regularly monitor adherence to information security policies and procedures through a combination of automated tools, internal audits, and management reviews. The Information Security Officer (ISO) is responsible for overseeing compliance monitoring activities, ensuring that controls are functioning as intended, and identifying instances of non-compliance. Findings from audits or assessments will be documented, and corrective actions will be initiated where necessary. Compliance metrics will be reported to executive management to support continuous improvement in the organization’s security posture.

### **Disciplinary Actions for Non-Compliance**

Violations of this Information Security Policy will be treated seriously and may result in disciplinary actions depending on the nature and severity of the breach. Disciplinary measures may include formal warnings, mandatory retraining, suspension of system access, or termination of employment or contracts. In cases where non-compliance results in legal or regulatory consequences, [Company Name] reserves the right to pursue legal action or notify relevant authorities. All disciplinary actions will be conducted in accordance with the company’s Human Resources policies and procedures, ensuring fairness and consistency.

## **17. Policy Review and Updates**

To ensure the continued relevance and effectiveness of the Information Security Policy, [Company Name] will establish a formal process for periodic reviews and updates. This process ensures that the policy remains aligned with evolving business needs, technological advancements, regulatory changes, and emerging security threats.

### **Review Schedule (Annually, As Needed)**

The Information Security Officer (ISO) is responsible for coordinating a comprehensive review of this policy at least once every 12 months. Additionally, reviews will be conducted on an as-needed basis in response to significant organizational changes, security incidents, audit findings, or modifications to applicable laws and regulations. The review process will involve key stakeholders, including executive management, IT leadership, and compliance officers, to ensure a thorough assessment of the policy's effectiveness and applicability.

### **Amendment Process**

Any updates or amendments to this policy must follow a formal change management process. Proposed changes will be documented, reviewed by the ISO, and submitted to executive management for approval. Once approved, the updated policy will be communicated to all employees, and training sessions will be arranged if necessary to address significant changes. The latest version of the policy will be made accessible through official company communication channels, and all personnel will be required to acknowledge their understanding of the revised policy.