**Information Security Policy**

**1. Purpose**

The purpose of this policy is to define the organization’s approach to protecting its information assets from threats that could compromise confidentiality, integrity, or availability. It establishes governance principles, defines responsibilities, and sets the tone for a culture of security across the organization.

**2. Scope**

This policy applies to:

* All employees, contractors, interns, consultants, and third parties with access to company systems or data.
* All forms of information (digital, printed, verbal, or otherwise).
* All devices and systems that store, process, or transmit company data, whether owned by the organization or used under bring-your-own-device (BYOD) arrangements.
* All business units, subsidiaries, and affiliates of the organization.

**3. Policy Objectives**

The organization’s information security program is designed to:

1. Protect sensitive and business-critical data from unauthorized access, alteration, disclosure, or destruction.
2. Ensure continuity of business operations in the face of disruptive events.
3. Demonstrate compliance with applicable legal, regulatory, and contractual obligations.
4. Embed secure practices into daily business activities, technology design, and vendor relationships.
5. Promote awareness and accountability so that every individual understands their role in protecting information.

**4. Security Principles**

The organization will adhere to the following core principles:

* **Confidentiality** – Access to information is restricted to authorized individuals on a need-to-know basis.
* **Integrity** – Data is accurate, complete, and protected from unauthorized modification.
* **Availability** – Information and systems are accessible when needed to support business functions.
* **Accountability** – Users and administrators are responsible for their actions and access.
* **Resilience** – Security controls are designed to anticipate, withstand, recover, and adapt to adverse conditions.

**5. Policy Requirements**

**5.1 Governance & Risk Management**

* A formal information security governance structure, led by the Chief Information Security Officer (CISO), will oversee the program.
* Risk assessments must be conducted regularly to identify and evaluate threats, vulnerabilities, and impacts.
* Risk treatment decisions must align with the organization’s risk appetite and be approved by leadership.
* All security policies must be reviewed annually and updated as needed.

**5.2 Access & Identity Management**

* Access to systems must follow the principle of least privilege.
* Multi-factor authentication (MFA) must be enforced for administrative accounts, remote access, and systems handling sensitive data.
* Privileged account use must be controlled, logged, and reviewed regularly.
* User accounts must be provisioned and deprovisioned promptly through established processes.

**5.3 Data Protection**

* Information must be classified based on sensitivity (e.g., Public, Internal, Confidential, Restricted).
* Data classified as Confidential or Restricted must be encrypted at rest and in transit using approved algorithms.
* Portable media must be encrypted or otherwise secured before transport.
* Sensitive information must not be stored or transmitted using unauthorized services (e.g., personal email, consumer cloud storage).

**5.4 Secure Systems & Development**

* Security must be embedded in the software development lifecycle (SDLC), including threat modeling, secure coding practices, and code review.
* All systems must be configured according to approved baselines and hardened to reduce attack surfaces.
* Vulnerabilities must be remediated within defined timelines based on severity.
* Logging, monitoring, and alerting must be enabled on critical systems to detect suspicious activity.

**5.5 Network & Infrastructure Security**

* Network perimeters must be protected by firewalls, intrusion detection/prevention systems, and segmentation.
* Remote access must use secure VPN or equivalent methods with encryption.
* Wireless networks must use strong authentication and encryption (e.g., WPA3 or enterprise-level WPA2).
* Administrative access to infrastructure must occur only through secure, monitored channels.

**5.6 Third-Party & Cloud Security**

* Vendors, partners, and service providers must undergo security due diligence before engagement.
* Contracts must include information security and privacy requirements.
* Cloud services must be approved and configured according to security standards, including identity integration and monitoring.

**5.7 Privacy & Compliance**

* Personal data must be processed in accordance with applicable data protection laws and the organization’s Privacy Policy.
* Any suspected data breach must be reported immediately to the Information Security team.
* Privacy impact assessments must be conducted for systems or projects handling personal or sensitive information.

**5.8 Asset & Equipment Management**

* All hardware, software, and data assets must be inventoried and tracked throughout their lifecycle.
* Disposal of equipment or media must follow secure destruction methods.
* Unauthorized hardware and software are prohibited from connecting to corporate networks.

**5.9 Security Awareness & Training**

* All employees must complete security awareness training upon hire and at least annually thereafter.
* Role-specific training must be provided for staff with elevated responsibilities (e.g., developers, system administrators).
* Phishing simulations and awareness campaigns will be conducted to strengthen employee vigilance.

**5.10 Incident Response & Business Continuity**

* A formal incident response plan must be maintained and tested at least annually.
* All employees are required to report suspected or actual security incidents immediately.
* Business continuity and disaster recovery plans must ensure critical operations can resume within defined recovery objectives.

**6. Roles & Responsibilities**

* **Board & Executive Leadership** – Approve security strategy and ensure adequate resources are allocated.
* **CISO** – Owns and maintains the information security program, policies, and risk reporting.
* **IT & Security Teams** – Implement controls, monitor compliance, and respond to incidents.
* **Managers** – Ensure teams comply with policies and report incidents promptly.
* **All Staff & Contractors** – Protect organizational assets, complete training, and comply with security requirements.

**7. Enforcement**

Failure to comply with this policy may result in disciplinary action, up to and including termination of employment or contract, and may also involve legal or regulatory consequences.

**8. Review Cycle**

This policy will be reviewed annually by the CISO, with approval from executive leadership. Revisions will be made sooner if required by changes in law, business operations, or the threat landscape.