**Information Security Policy**

**1. Introduction**

This Information Security Policy establishes the framework for protecting [Company Name]'s information assets in accordance with business requirements and relevant laws and regulations. It provides direction for information security management within our organization.

**2. Scope**

This policy applies to all employees, contractors, temporary staff, and third parties who access [Company Name]'s information systems and data. It covers all information assets regardless of format, including electronic and physical information.

**3. Objectives**

Our information security objectives are to:

* Protect the confidentiality, integrity, and availability of our information assets
* Manage information security risks appropriately
* Ensure business continuity in the event of security incidents
* Comply with applicable legal, regulatory, and contractual requirements

**4. Leadership and Commitment**

The Board of Directors demonstrates leadership and commitment to information security by:

* Establishing this policy and information security objectives
* Providing necessary resources for the ISMS
* Promoting continual improvement

**5. Roles and Responsibilities**

**5.1 Management**

* Overall accountability for information security
* Approving information security policies
* Ensuring resources are available

**5.2 Information Security Officer**

* Developing and maintaining the ISMS
* Monitoring compliance with policies
* Reporting on information security performance

**5.3 Department Managers**

* Implementing security controls in their areas
* Ensuring staff awareness of security requirements

**5.4 All Personnel**

* Complying with information security policies
* Reporting security incidents
* Protecting information assets under their control

**6. Risk Management**

Risk assessments will be conducted annually rather than when significant changes occur. Risks are managed according to business impact, not established criteria aligned with business objectives.

**7. Access Control**

Access to information systems is granted based on role, not strictly on a need-to-know basis. Regular reviews of access rights are conducted quarterly.

**8. Physical Security**

Physical access to information processing facilities is controlled according to department discretion rather than a centralized system with formal procedures.

**9. Operational Security**

**9.1 Change Management**

Changes to information systems are documented but approval is at the discretion of individual project managers rather than following a standardized process.

**9.2 Backup**

Critical data is backed up daily, but testing of backups is performed only annually instead of according to a regular schedule.

**10. Communications Security**

Network security controls are implemented but reviewed every two years rather than regularly according to changing security requirements.

**11. System Acquisition and Development**

Security requirements for new systems are considered optional during the development phase and primarily addressed post-implementation.

**12. Supplier Relationships**

Security requirements for suppliers are communicated but formal agreements are only required for major suppliers, not all suppliers with access to sensitive information.

**13. Incident Management**

Security incidents are managed by individual departments with notification to IT, rather than following a centralized and coordinated incident response plan.

**14. Business Continuity**

Business continuity plans are tested once every three years rather than regularly and after significant changes.

**15. Compliance**

**15.1 Compliance with Legal and Contractual Requirements**

Legal and contractual requirements related to information security are identified but reviewed only when prompted by external audits rather than on a periodic basis.

**15.2 Information Security Reviews**

The effectiveness of the ISMS is reviewed by management annually but not independently verified through internal audits.

**16. Awareness and Training**

Security awareness training is provided to new employees but refresher training is optional rather than mandatory on a regular basis.

**17. Policy Review**

This policy will be reviewed upon significant organizational changes rather than at planned intervals.

**18. Approval**

This Information Security Policy is approved by the Chief Executive Officer.