MINISTRY OF SECURITY

INFORMATION SECURITY POLICY

INLINE WITH ISO 27001, SOC2 & NIST CSF

Prepared by :

INFORMATION SECURITY POLICY

Document Control

Policy Owner: Chief Information Security Officer
Version: 1.0
Last Updated: [Date]
Review Cycle: Annual
Classification: Internal
Status: [Draft/Approved]
Next Review Date: [Date]

1. Purpose

This Information Security Policy establishes the framework for protecting [Organization Name]'s information assets. It demonstrates management's commitment to implementing, maintaining, and continuously improving information security within the organization. This policy serves as the cornerstone document that defines the organization's approach to information security management and provides the basis for all subordinate information security procedures and standards.

2. Scope

This policy applies to all information assets owned, operated, or managed by [Organization Name], regardless of location or format. This includes all employees, contractors, consultants, temporary staff, and third-party entities who have access to, or responsibility for, [Organization Name]'s information assets. The policy encompasses all information systems, applications, infrastructure, business processes, and physical facilities involved in the processing, storage, and transmission of information.

3. Information Security Policy Statements

3.1 Information Security Management System (ISMS)

[Organization Name] shall establish, implement, maintain, and continually improve an Information Security Management System in accordance with ISO/IEC 27001:2013. The ISMS shall encompass all business functions, locations, and information assets within the defined scope. Management shall demonstrate leadership and commitment by ensuring the integration of information security requirements into the organization's business

processes, providing necessary resources, and promoting continuous improvement. The effectiveness of the ISMS shall be measured through defined metrics, reviewed at planned intervals, and reported to senior management at least quarterly. All employees and relevant external parties shall be made aware of their role in maintaining the effectiveness of the ISMS through regular communication and training programs.

3.2 Risk Management

The organization shall implement and maintain a comprehensive risk management framework that identifies, assesses, and treats information security risks in alignment with business objectives and stakeholder requirements. Risk assessments shall be conducted at planned intervals, at least annually, and whenever significant changes to the business environment, technology infrastructure, or threat landscape occur. The risk assessment methodology shall consider both threats and vulnerabilities, evaluate potential impacts to confidentiality, integrity, and availability of information, and document the rationale for risk treatment decisions. Risk treatment plans shall be developed and implemented based on the organization's defined risk acceptance criteria, with regular monitoring and reporting of risk treatment effectiveness to relevant stakeholders.

3.3 Access Control Management

[Organization Name] shall implement and maintain a comprehensive access control framework based on the principles of least privilege and need-to-know. All access to information systems and data shall be controlled through formal user registration and de-registration procedures. Access rights shall be granted only after documented approval from both the resource owner and the information security team. Multi-factor authentication shall be mandatory for all remote access and privileged account access. Regular access reviews shall be conducted at least quarterly, with immediate revocation of access rights upon termination or role change. The organization shall maintain audit logs of all access control changes, with automated alerts for suspicious access attempts or unauthorized privilege escalations. Password policies shall enforce strong authentication requirements including minimum length, complexity, and regular password changes, with technical controls preventing password reuse.

3.4 Asset Management and Classification

The organization shall maintain a comprehensive inventory of all information assets, including both physical and logical assets, with clearly assigned ownership and defined security responsibilities. All information assets shall be classified according to their sensitivity, criticality, and legal requirements using the organization's defined classification scheme. Asset owners shall be responsible for ensuring appropriate handling procedures are implemented based on the asset's classification level. The asset inventory shall be reviewed and updated at least quarterly, with formal reconciliation processes to identify and address any discrepancies. Media handling procedures shall be implemented to protect against unauthorized disclosure, modification, or destruction throughout the asset lifecycle, including secure storage, transmission, and disposal methods.

3.5 Cryptography and Key Management

[Organization Name] shall implement and maintain cryptographic controls to protect the confidentiality, integrity, and authenticity of information throughout its lifecycle. All sensitive data shall be encrypted both in transit and at rest using industry-standard encryption algorithms and protocols. The organization shall maintain a formal key management policy covering the entire cryptographic key lifecycle, including generation, distribution, storage, use, archival, and destruction. Cryptographic keys shall be protected against unauthorized access, loss, and compromise through the use of hardware security modules (HSMs) or equivalent secure key storage mechanisms. Regular assessments of cryptographic implementations shall be conducted to ensure alignment with current industry standards and best practices, with documented procedures for transitioning to stronger cryptographic controls when required.

3.6 Physical and Environmental Security

The organization shall implement and maintain appropriate physical and environmental security controls to prevent unauthorized physical access, damage, theft, compromise, or interference to information assets and information processing facilities. Security perimeters shall be clearly defined and protected through layered security controls including access card systems, surveillance cameras, and security personnel where appropriate. All physical access shall be logged and monitored, with regular reviews of access logs and immediate investigation of security incidents. Environmental controls shall be implemented to protect against environmental threats such

as fire, flood, or power failure, with regular testing and maintenance of all environmental protection systems. Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel can gain access, with additional controls for areas containing sensitive information or critical systems.

3.7 Operations Security

[Organization Name] shall establish and maintain documented operating procedures for all information processing facilities to ensure correct and secure operations. Change management procedures shall be implemented to control all changes to information processing facilities and systems, with appropriate testing, documentation, and approval requirements. Development, testing, and operational environments shall be separated to reduce the risks of unauthorized access or changes to operational systems. System and security monitoring controls shall be implemented to detect unauthorized information processing activities, with regular review and analysis of system logs. Protection against malware shall be implemented through a defense-in-depth approach including endpoint protection, email filtering, web filtering, and regular security awareness training for all users.

3.8 Communications Security

The organization shall implement and maintain controls to ensure the security of information in networks and its supporting information processing facilities. Network security controls shall include network segregation, encryption of sensitive traffic, regular vulnerability assessments, and intrusion detection/prevention systems. All external network connections shall be identified, documented, and secured through formal agreements that include specific security requirements. Information transfer policies and procedures shall be established to protect the transfer of information through the use of all types of communication facilities, including requirements for encryption, digital signatures, and non-repudiation where appropriate.

3.9 System Acquisition, Development, and Maintenance

Security requirements shall be identified and integrated into all stages of the system development lifecycle, from planning and design through implementation and maintenance. All new systems or significant changes to existing systems shall undergo security testing and formal security review before deployment to production environments. Secure development

principles shall be followed, including input validation, output encoding, and secure session management. Regular vulnerability assessments and penetration testing shall be conducted on all systems, with timely remediation of identified vulnerabilities based on risk assessment.

3.10 Supplier Relationships

The organization shall establish and maintain information security requirements for relationships with suppliers to mitigate risks associated with supplier access to organizational assets. Formal contracts or agreements shall include specific security requirements, including incident reporting obligations, data protection requirements, and right-to-audit clauses. Supplier service delivery shall be regularly monitored and reviewed, with formal assessments of security controls implemented by suppliers conducted at least annually. Changes to supplier services shall be managed through formal change management procedures, with impact assessments conducted for significant changes.

3.11 Information Security Incident Management

[Organization Name] shall implement and maintain an information security incident management process to ensure a consistent and effective approach to the management of information security incidents. All employees and contractors shall be required to report any observed or suspected security incidents immediately through defined reporting channels. The incident response team shall be properly trained and equipped to handle various types of security incidents, with defined procedures for incident detection, reporting, assessment, response, and recovery. Lessons learned from security incidents shall be documented and used to improve security controls and incident response procedures. Regular testing of incident response procedures shall be conducted through tabletop exercises and simulated incidents.

3.12 Business Continuity Management

The organization shall develop, maintain, and regularly test business continuity plans to ensure the continued availability of critical information processing facilities. Business impact analyses shall be conducted to identify critical business functions and their dependencies on information systems. Recovery time objectives (RTOs) and recovery point objectives (RPOs) shall be defined for all critical systems and processes. Regular backup procedures shall be implemented with periodic testing of backup restoration. Alternative

processing facilities shall be identified and maintained to support business continuity requirements, with regular testing of failover procedures.

SECTION 4: ROLES AND RESPONSIBILITIES

4.1 Board of Directors

The Board of Directors shall provide strategic oversight of the organization's information security program and demonstrate organizational commitment to information security through:

- Annual review and approval of the Information Security Policy and significant security initiatives
- Ensuring adequate resources are allocated to the information security program
- Oversight of significant security risks and incidents through regular reporting
- Review of annual security program effectiveness metrics and assessments
- Approval of the organization's risk appetite and tolerance levels related to information security

4.2 Executive Management

Executive Management, including the CEO and executive leadership team, shall be responsible for:

- Establishing and maintaining a strong security culture throughout the organization
- Approving information security strategies, policies, and major initiatives
- Ensuring information security requirements are integrated into organizational processes
- Allocating sufficient resources (financial, human, and technical) to maintain effective security controls
- Reviewing security performance metrics and risk indicators quarterly
- Supporting cross-functional coordination for security initiatives
- Ensuring security considerations are included in business planning and decision-making

4.3 Chief Information Security Officer (CISO)

The CISO shall have direct operational responsibility for the information security program and shall:

- Develop and maintain the organization's information security strategy and policies

- Oversee the implementation and operation of security controls across the organization
- Report security status, risks, and significant issues to executive management and the Board
- Manage the information security team and security operations
- Ensure compliance with security requirements and standards
- Coordinate security incident response activities
- Maintain relationships with external security partners and stakeholders
- Lead security awareness and training programs
- Provide security expertise and guidance to business units
- Review and approve security architecture and designs

4.4 Information Security Team

The Information Security Team, under the direction of the CISO, shall:

- Implement and maintain security controls according to approved policies
- Monitor security events and respond to security incidents
- Conduct security assessments, audits, and testing
- Provide security consulting to business units and projects
- Manage security tools and technologies
- Develop security procedures and guidelines
- Deliver security awareness training
- Perform security risk assessments
- Support compliance activities and audits
- Investigate security incidents and violations

4.5 Department Managers and Business Unit Leaders

Department Managers and Business Unit Leaders shall be responsible for:

- Implementing security controls within their areas of responsibility
- Ensuring staff compliance with security policies and procedures
- Identifying and communicating security requirements for business processes
- Supporting security risk assessments and audits
- Reporting security incidents promptly
- Maintaining asset inventory for their department
- Reviewing access rights for their staff regularly
- Incorporating security requirements into project planning
- Supporting security awareness within their teams
- Ensuring security considerations in vendor relationships

4.6 System and Data Owners

System and Data Owners shall be accountable for:

- Defining classification levels for their information assets
- Approving access to systems and data under their ownership
- Reviewing access rights periodically
- Ensuring appropriate security controls are implemented
- Participating in risk assessments and security reviews
- Defining backup and recovery requirements
- Approving system changes that affect security
- Supporting security incident investigations
- Maintaining documentation of system security requirements
- Ensuring compliance with security policies for their assets

4.7 All Employees, Contractors, and Third Parties

All individuals who have access to organizational information assets shall:

- Comply with all information security policies and procedures
- Complete required security awareness training
- Protect information assets under their control
- Report security incidents and violations promptly
- Use information assets only for authorized purposes
- Maintain confidentiality of sensitive information
- Follow secure working practices
- Protect authentication credentials
- Ensure physical security of assets
- Support security assessments and audits as required

SECTION 5: COMPLIANCE AND ENFORCEMENT

5.1 Compliance Requirements

5.1.1 Policy Compliance

All employees, contractors, and third parties shall comply with this Information Security Policy and all supporting policies, procedures, and standards. Compliance shall be monitored through:

- Regular security assessments and audits
- Automated compliance monitoring tools
- Security metrics and reporting
- Access reviews and activity logs
- Security awareness assessments
- Vendor security assessments
- Compliance validation processes

5.1.2 Regulatory Compliance

The organization shall maintain compliance with all applicable laws, regulations, and contractual obligations related to information security, including but not limited to:

- Industry-specific regulations
- Data protection and privacy laws
- Security breach notification requirements
- Electronic transaction regulations
- Records retention requirements
- Export control regulations
- Intellectual property protection

5.1.3 Compliance Monitoring

The Information Security Team shall implement and maintain processes to monitor compliance with security requirements through:

- Automated security configuration monitoring
- Regular vulnerability assessments
- Security control testing
- Log monitoring and analysis
- Access control reviews
- Security metrics collection
- Compliance assessments
- Third-party security reviews

5.1.4 Audit Requirements

Internal and external security audits shall be conducted regularly to verify compliance with this policy and supporting requirements:

- Internal security audits shall be conducted at least annually
- External security audits shall be conducted every two years
- Specialized audits shall be conducted as required by regulations
- Audit findings shall be tracked to resolution
- Audit reports shall be provided to appropriate management
- Remediation plans shall be developed for identified gaps

5.2 Policy Enforcement

5.2.1 Violations

Security policy violations shall be handled according to established procedures:

- All suspected violations shall be investigated promptly
- Investigations shall be conducted by authorized personnel
- Evidence shall be collected and preserved appropriately
- Confidentiality shall be maintained during investigations
- Results shall be documented and reported to management
- Appropriate corrective actions shall be implemented

5.2.2 Disciplinary Actions

Violations of this policy may result in disciplinary action up to and including termination of employment or contract:

- Disciplinary actions shall be determined based on:
  - Severity of the violation
  - Intent of the violator
  - Impact on the organization
  - History of previous violations
  - Cooperation with investigation
- Disciplinary actions shall be:
  - Consistently applied
  - Properly documented
  - Reviewed by appropriate parties
  - Communicated as appropriate
  - Implemented promptly

5.2.3 Appeals Process

Individuals subject to disciplinary action shall have the right to appeal:

- Appeals must be submitted in writing within 5 business days
- Appeals shall be reviewed by designated authorities
- Additional information may be requested during review
- Appeal decisions shall be documented and communicated
- Appeal decisions shall be final

5.2.4 Legal Actions

The organization reserves the right to pursue legal action for policy violations that:

- Result in significant harm or loss
- Violate applicable laws or regulations
- Breach contractual obligations
- Involve criminal activities
- Require regulatory reporting

5.3 Compliance Reporting

5.3.1 Internal Reporting

Regular compliance reporting shall be provided to management:

- Monthly security metrics and compliance indicators
- Quarterly compliance status reports to executive management
- Annual compliance assessment reports to the Board
- Ad-hoc reporting of significant compliance issues
- Trend analysis and recommendations

5.3.2 External Reporting

External compliance reporting shall be provided as required:

- Regulatory compliance reports
- Customer compliance attestations
- Audit reports for external parties
- Security incident notifications
- Breach reporting as required by law

5.3.3 Compliance Documentation

All compliance activities shall be documented and retained:

- Assessment and audit reports
- Compliance monitoring results
- Investigation records
- Disciplinary action records
- Remediation plans and status
- Training and awareness records

SECTION 6: EXCEPTIONS AND DEVIATIONS

6.1 Exception Request Process

The organization recognizes that legitimate business needs may occasionally require exceptions to this policy. All exceptions shall be managed through a formal process:

6.1.1 Exception Request Requirements

Exception requests must include:

- Detailed description of the requested exception
- Business justification and impact analysis
- Risk assessment and proposed compensating controls
- Implementation timeline and duration
- Technical specifications if applicable
- Cost-benefit analysis
- System and data owners' approval

6.1.2 Exception Review and Approval

All exception requests shall follow a structured review and approval process:

- Initial review by Information Security Team
- Risk assessment validation
- Technical review if required
- Approval by appropriate authority based on risk level:
  - Low risk: CISO approval
  - Medium risk: CISO and CIO approval
  - High risk: Executive Management approval
  - Critical risk: Board level approval

6.1.3 Exception Documentation

All approved exceptions shall be documented including:

- Unique exception identifier
- Scope and duration of exception
- Approved compensating controls
- Implementation requirements
- Monitoring and review requirements
- Approval signatures and dates

6.2 Exception Management

6.2.1 Exception Tracking

The Information Security Team shall maintain an exception register containing:

- All current and historical exceptions
- Status of compensating controls
- Exception expiration dates
- Review and renewal dates
- Risk reassessment results
- Compliance implications

6.2.2 Exception Monitoring

Approved exceptions shall be monitored to ensure:

- Compensating controls remain effective
- Business justification remains valid
- Risk levels haven't changed
- Compliance requirements are met
- Exception duration isn't exceeded

6.2.3 Exception Review and Renewal

All exceptions shall be reviewed:

- At least quarterly for high and critical risk exceptions
- At least semi-annually for medium risk exceptions
- Annually for low risk exceptions
- Prior to expiration date
- When significant changes occur

SECTION 7: REVIEW AND MAINTENANCE

7.1 Policy Review Process

7.1.1 Regular Review

This policy shall be reviewed:

- At least annually
- When significant organizational changes occur
- After major security incidents

- When new threats or vulnerabilities are identified
- When regulatory requirements change
- When technology changes impact security requirements

7.1.2 Review Participants

Policy reviews shall include participation from:

- Information Security Team
- Legal Department
- Compliance Team
- IT Department
- Business Unit Representatives
- Risk Management
- External Subject Matter Experts (as needed)

7.1.3 Review Criteria

Policy reviews shall evaluate:

- Effectiveness of current controls
- Alignment with business objectives
- Compliance with regulations
- Relevance to current threats
- Implementation challenges
- Resource requirements
- User feedback
- Incident lessons learned

7.2 Policy Maintenance

7.2.1 Policy Updates

Updates to this policy shall:

- Follow change management procedures
- Be documented with version control
- Include summary of changes
- Be reviewed by stakeholders
- Receive appropriate approvals
- Be communicated effectively

7.2.2 Supporting Documentation

Related documents shall be maintained including:

- Procedures and guidelines
- Technical standards
- Implementation guides
- Training materials
- Assessment tools
- Compliance checklists

7.2.3 Communication and Training

Policy changes shall be:

- Communicated to all affected parties
- Incorporated into training programs
- Posted in accessible locations
- Included in awareness campaigns
- Verified for understanding

APPENDIX A: DEFINITIONS

A.1 General Terms

- **Information Security**: The protection of information from a wide range of threats in order to ensure business continuity, minimize business risk, and maximize return on investments and business opportunities.
- **Information Security Management System (ISMS)**: A systematic approach for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an organization's information security.
- **Risk**: The potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization.
- **Control**: Means of managing risk, including policies, procedures, guidelines, practices, or organizational structures, which can be of administrative, technical, management, or legal nature.

A.2 Technical Terms

- **Authentication**: The process of verifying the claimed identity of a user, process, or device.
- **Authorization**: The process of granting or denying specific requests for obtaining and using information resources.
- **Encryption**: The process of converting information into a form unintelligible to anyone except holders of a specific cryptographic key.
- **Incident**: A single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations.

A.3 Classification Terms

- **Public Information**: Information that has been declared public knowledge and can be freely distributed.
- **Internal Information**: Information that is intended for use within the organization and unauthorized disclosure would be against policy.
- **Confidential Information**: Information that requires special precautions to protect it from unauthorized disclosure.
- **Restricted Information**: The most sensitive business information, intended strictly for use within specific groups.

APPENDIX B: RELATED DOCUMENTS

B.1 Policies

- Access Control Policy
- Asset Management Policy
- Business Continuity Policy
- Cryptography Policy
- Data Protection Policy
- Incident Management Policy
- Network Security Policy
- Physical Security Policy
- Remote Working Policy
- Supplier Security Policy

B.2 Procedures

- Access Management Procedures
- Backup and Recovery Procedures
- Change Management Procedures
- Incident Response Procedures
- System Development Procedures
- Vulnerability Management Procedures

B.3 Standards

- Configuration Standards
- Encryption Standards
- Network Security Standards
- Password Standards
- System Hardening Standards

B.4 Guidelines

- Data Classification Guidelines
- Risk Assessment Guidelines
- Secure Development Guidelines
- Security Testing Guidelines
- Third-Party Security Guidelines

APPENDIX C: REFERENCES

C.1 International Standards

- ISO/IEC 27001:2013 - Information Security Management Systems Requirements
- ISO/IEC 27002:2013 - Code of Practice for Information Security Controls
- ISO/IEC 27005:2018 - Information Security Risk Management

C.2 Regulatory Requirements

- [List applicable regulations]
- [Industry-specific requirements]
- [Regional requirements]

C.3 Best Practices

- NIST Cybersecurity Framework
- CIS Controls
- OWASP Security Guidelines
- Cloud Security Alliance Guidelines

APPENDIX D: DOCUMENT HISTORY

D.1 Version Control

Version	Date	Author	Approver	Description of Changes
1.0	[Date]	[Name]	[Name]	Initial Release

D.2 Review History

Review Date	Reviewer	Outcome	Next Review
[Date]	[Name]	[Outcome]	[Date]

APPENDIX E: FORMS AND TEMPLATES

E.1 Required Forms

- Exception Request Form
- Security Incident Report Form
- Access Request Form
- Risk Assessment Template
- Audit Checklist Template
- Policy Acknowledgment Form

E.2 Supporting Templates

- Security Design Review Template
- Vendor Security Assessment Template
- Business Impact Analysis Template
- Project Security Plan Template
- Security Metrics Scorecard Template

DID YOU FIND THIS DOCUMENT USEFUL

FOLLOW FOR FREE INFOSEC CHECKLISTS | PLAYBOOKS TRAININGS | VIDEOS

WWW.MINISTRYOFSECURITY.CO