ISMS Manual

DOCUMENT CLASSIFICATION	Internal
VERISON	1.0
DATE	
DOCUMENT AUTHOR	**Ayaz Sabir**
DOCUMENT OWNER	

REVISION HISTORY

VERSION	DATE	REVISION AUTHOR	SUMMARY OF CHANGES

DISTRIBUTION LIST

NAME	SUMMARY OF CHANGE

APPROVAL

NAME	POSITION	SIGN

Contents

1. Introduction

This Information Security Management System (ISMS) Manual serves as the primary documented guide for your organization's approach to managing information security. It has been developed to meet the requirements of the ISO/IEC 27001:2022 standard and to provide a framework for protecting the confidentiality, integrity, and availability of information assets. The purpose of this manual is to:

- Define the scope of the ISMS, including its boundaries and applicability within the organization.
- Establish a clear and consistent framework for managing information security risks.
- Document the policies, procedures, and controls that support the ISMS.
- Communicate the organization's commitment to information security to all stakeholders, including employees, customers, partners, and regulatory bodies.
- Provide a basis for auditing and assessing the effectiveness of the ISMS.

The scope of this ISMS Manual applies to all employees, contractors, and third-party service providers who have access to your organization's information assets. It covers all business processes, information systems, and physical locations that are critical to the organization's operations and are included within the defined scope of the ISMS.

2. Context of the Organization (Clause 4)

2.1 Understanding the Organization and its Context

your organization has established a comprehensive understanding of its internal and external context to ensure that the ISMS is aligned with its strategic objectives and the needs of its stakeholders. This involves identifying and analyzing various factors that can influence the effectiveness of the ISMS, including:

- Internal Context: This includes the organization's culture, policies, objectives, governance, roles and responsibilities, and information systems. We have considered our organizational structure, business processes, and the resources available to support the ISMS.
- External Context: This includes the social, cultural, political, legal, regulatory, financial, technological, economic, and competitive environment in which the organization operates. We have analyzed the market trends, customer expectations, and the threat landscape to identify potential risks and opportunities.

2.2 Understanding the Needs and Expectations of Interested Parties

your organization has identified its interested parties and their requirements related to information security. This includes, but is not limited to:

- **Customers**: Expect their data to be protected and their privacy to be respected.
- **Employees**: Require a secure working environment and clear guidelines on information security.
- **Shareholders and Investors**: Expect the organization to manage information security risks effectively to protect their investments.
- **Regulators and Government Agencies**: Require compliance with applicable laws and regulations.
- **Suppliers and Partners**: Expect secure collaboration and protection of shared information.

A list of interested parties and their requirements is maintained in the Appendices.

2.3 Determining the Scope of the Information Security Management System

The scope of the ISMS has been defined to cover all critical information, assets, business processes, and locations that are essential for your organization's operations. The scope is documented in the ISMS Scope Statement, which is reviewed and updated as necessary.
The scope statement clearly defines the boundaries of the ISMS and the interfaces with external entities.

2.4 Information Security Management System

your organization has established, implemented, maintained, and will continually improve an ISMS in accordance with the requirements of ISO/IEC 27001:2022. The ISMS is an integral part of our overall business management system and is designed to be flexible and scalable to adapt to changes in our business environment.

3. Leadership (Clause 5)

3.1 Leadership and Commitment

Top management at your organization is committed to the effectiveness of the ISMS. This commitment is demonstrated by:

Ensuring that the information security policy and objectives are established and are

compatible with the strategic direction of the organization.

- Integrating the ISMS requirements into the organization's business processes.
- Providing the necessary resources for the ISMS.
- Communicating the importance of effective information security management and of conforming to the ISMS requirements.
- Ensuring that the ISMS achieves its intended outcomes.
- Directing and supporting persons to contribute to the effectiveness of the ISMS.
- Promoting continual improvement.

3.2 Policy

Top management has established an information security policy that is appropriate to the purpose of the organization. The policy is communicated within the organization and is available to interested parties as appropriate. The information security policy is reviewed at planned intervals or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.

3.3 Organizational Roles, Responsibilities and Authorities

Top management has assigned and communicated the responsibilities and authorities for roles relevant to information security. The Information Security Manager is responsible for the overall implementation and maintenance of the ISMS. All managers are responsible for implementing the information security policy in their respective areas. All employees are responsible for complying with the information security policy and procedures.

4. Planning (Clause 6)

4.1 Actions to Address Risks and Opportunities

your organization has established a systematic process for identifying, analyzing, and evaluating information security risks. This process is based on a formal risk assessment methodology that is documented in the Appendices. The risk assessment process considers the threats to our information assets, the vulnerabilities of our systems, and the impact that a security incident could have on our business operations. We also consider opportunities for improving our information security posture.

4.2 Information Security Objectives and Planning to Achieve Them

your organization has established information security objectives at relevant functions and levels. These objectives are consistent with the information security policy and are measurable. We have also developed plans to achieve these objectives, including the resources required, the responsibilities assigned, and the timelines for completion. The information security objectives are reviewed and updated as necessary to ensure their continued relevance and effectiveness.

5. Support (Clause 7)

5.1 Resources

your organization is committed to providing the necessary resources to establish, implement, maintain, and continually improve the ISMS. This includes providing sufficient personnel with the required skills and expertise, as well as the necessary technology and financial resources.

5.2 Competence

your organization ensures that all personnel involved in the ISMS are competent on the basis of appropriate education, training, or experience. We have established a process for identifying the training needs of our employees and for providing the necessary training to ensure that they have the skills and knowledge required to perform their roles effectively.

5.3 Awareness

your organization has established a security awareness program to ensure that all employees are aware of the information security policy, their responsibilities, and the importance of their contribution to the effectiveness of the ISMS. The awareness program includes regular training sessions, newsletters, and other forms of communication.

5.4 Communication

your organization has established a communication plan to ensure that information related to the ISMS is communicated effectively to all relevant internal and external parties. The communication plan defines what will be communicated, when, to whom, and how. A summary of the communication plan is included in the Appendices.

5.5 Documented Information

your organization maintains documented information to support the ISMS. This includes the information security policy, objectives, risk assessment and treatment plans, procedures, and records. All documented information is controlled to ensure its availability, integrity, and confidentiality.

6. Operation (Clause 8)

6.1 Operational Planning and Control

your organization plans, implements, and controls the processes needed to meet information security requirements and to implement the actions determined in Clause 6. This includes the management of outsourced processes that are relevant to the ISMS. We have established criteria for the processes and have implemented controls to ensure that the processes are carried out as planned.

6.2 Information Security Risk Assessment

your organization conducts information about security risk assessments at planned intervals and when significant changes occur. The risk assessment process is systematic and is based on the methodology documented in the Appendices. The results of the risk assessment are used to identify the risks that need to be treated.

6.3 Information Security Risk Treatment

your organization has developed a risk treatment plan to address the risks identified in the risk assessment. The risk treatment plan includes the selection of appropriate controls from Annex A of the ISO/IEC 27001:2022 standard, as well as the implementation of other risk treatment options, such as risk avoidance, risk transfer, or risk acceptance. The Statement of Applicability (SoA) documents the controls that have been selected and the justification for their inclusion.

7. Performance Evaluation (Clause 9)

7.1 Monitoring, Measurement, Analysis and Evaluation

your organization has established a process for monitoring, measuring, analyzing, and evaluating the performance of the ISMS. This includes monitoring the effectiveness of the controls, measuring the achievement of the information security objectives, and analyzing the trends in security incidents. The results of the performance evaluation are used to identify areas for improvement.

7.2 Internal Audit

your organization conducts internal audits at planned intervals to provide information on whether the ISMS conforms to the organization's own requirements for its ISMS and the requirements of ISO/IEC 27001:2022. The audit program is planned, taking into consideration the results of previous audits and the importance of the processes concerned. The audit results are reported to relevant management.

7.3 Management Review

Top management reviews the ISMS at planned intervals to ensure its continuing suitability, adequacy, and effectiveness. The management review includes an assessment of opportunities for improvement and the need for changes to the ISMS, including the information security policy and objectives. The results of the management review are documented.

8. Improvement (Clause 10)

8.1 Nonconformity and Corrective Action

your organization has established a process for identifying and managing nonconformities and for taking corrective action to eliminate the cause of the nonconformity. The process includes a review of the nonconformity, an investigation of the cause, and the implementation of corrective action to prevent recurrence. The effectiveness of the corrective action is reviewed.

8.2 Continual Improvement

your organization is committed to continually improving the suitability, adequacy, and effectiveness of the ISMS. We use the results of the performance evaluation, internal audits, and management reviews to identify opportunities for improvement. We also consider changes in our internal and external context and the needs and expectations of our interested parties when planning for continually improving the ISMS.

9. Annex A: Information Security Controls Reference

This annex provides a reference to the information security controls selected by your organization to mitigate the identified risks. The selection of controls is based on the results of the risk assessment and is documented in the Statement of Applicability (SoA).

9.1 Statement of Applicability (SoA)

The Statement of Applicability (SoA) is a key document in the ISMS. It lists all the controls from Annex A of the ISO/IEC 27001:2022 standard and indicates whether each control is applicable to our organization. For each applicable control, the SoA provides a justification for its inclusion and a reference to the relevant documentation that describes how the control is implemented. For each control that is not applicable, SoA provides a justification for its exclusion.

SoA is a controlled document and is reviewed and updated as necessary to reflect changes in our risk environment or business requirements.

9.2 Organizational Controls (A.5)

This section provides a summary of the organizational controls that have been implemented by your organization to manage information security.

A.5.1 Policies for Information Security

Control: Information security policies shall be defined, approved by management, published, and communicated to employees and relevant external parties.

Implementation: your organization has established a comprehensive set of information security policies that are aligned with our business objectives and the requirements of the ISO/IEC 27001:2022 standard. These policies are reviewed and approved by top management and are communicated to all employees through our security awareness program. The policies are also made available to relevant external parties as appropriate.

A.5.2 Information Security Roles and Responsibilities

Control: Information security roles and responsibilities shall be defined and allocated.

Implementation: your organization has defined and allocated the roles and responsibilities for information security. The Information Security Manager is responsible for the overall implementation and maintenance of the ISMS. All managers are responsible for implementing the information security policy in their respective areas. All employees are responsible for complying with the information security policy and procedures.

A.5.3 Segregation of Duties

Control: Conflicting duties and areas of responsibility shall be segregated.

Implementation: your organization has implemented segregation of duties to reduce the risk of unauthorized or unintentional modification or misuse of our assets. We have identified

and segregated conflicting duties and have implemented controls to ensure that no single individual has excessive control over our critical processes.

A.5.4 Management Responsibilities

Control: Management shall require all employees and contractors to apply information security in accordance with the established information security policy, topic-specific policies and procedures of the organization.

Implementation: Management at your organization is committed to ensuring that all employees and contractors are aware of their information security responsibilities and that they comply with our information security policies and procedures. This is achieved through regular communication, training, and monitoring.

A.5.5 Contact With Authorities

Control: The organization shall establish and maintain contact with relevant authorities.

Implementation: your organization has established and maintains contact with relevant authorities, such as law enforcement agencies and regulatory bodies. This ensures that we are aware of our legal and regulatory obligations and that we can respond effectively to security incidents.

A.5.6 Contact With Special Interest Groups

Control: The organization shall establish and maintain contact with special interest groups or other specialist security forums and professional associations.

Implementation: your organization maintains contact with special interest groups and other specialist security forums to stay informed about the latest security threats, vulnerabilities, and best practices. This helps us to continually improve our information security posture.

A.5.7 Threat Intelligence

Control: Information relating to information security threats shall be collected and analyzed to produce threat intelligence.

Implementation: your organization has implemented a process for collecting and analyzing information about information security threats. This includes monitoring public and private sources of threat intelligence, as well as analyzing our own security incidents. The threat intelligence produced is used to inform our risk assessment and risk treatment processes.

A.5.8 Information Security in Project Management

Control: Information security shall be integrated into project management.

Implementation: your organization has integrated information security into our project management methodology. This ensures that information security risks are identified and addressed throughout the project lifecycle. All projects are required to have a security plan that is reviewed and approved by the Information Security Manager.

A.5.9 Inventory of Information and Other Associated Assets

Control: An inventory of information and other associated assets, including owners, shall be identified and maintained.

Implementation: your organization has established and maintains an inventory of our information and other associated assets. The inventory includes information about the owner, location, and classification of each asset. The inventory is reviewed and updated regularly to ensure its accuracy.

A.5.10 Acceptable Use of Information and Other Associated Assets

Control: Rules for the acceptable use of information and other associated assets shall be identified, documented, and implemented.

Implementation: your organization has established rules for the acceptable use of our information and other associated assets. These rules are documented in our acceptable use policy, which is communicated to all employees. The acceptable use policy is enforced through technical and administrative controls.

A.5.11 Return of Assets

Control: All employees and external party users shall return all of the organization's assets in their possession upon termination of their employment, contract or agreement.

Implementation: your organization has a formal process for the return of assets upon termination of employment, contract, or agreement. This process ensures that all assets, including laptops, mobile devices, and access cards, are returned in a timely manner. The process is documented in our employee offboarding procedure.

A.5.12 Classification of Information

Control: Information shall be classified in terms of legal requirements, value, criticality and sensitivity to unauthorized disclosure or modification.

Implementation: your organization has established a data classification scheme to ensure

that information is protected according to its value, criticality, and sensitivity. The classification scheme includes four levels: Public, Internal, Confidential, and Restricted. All information is classified and handled according to the requirements of its classification level.

A.5.13 Labelling of Information

Control: An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by the organization.

Implementation: your organization has implemented procedures for the labelling of information according to its classification. This includes the use of labels in email subjects, document headers and footers, and on physical media. The labelling procedures are documented in our data handling standard.

A.5.14 Information Transfer

Control: Information transfer rules, procedures, and agreements shall be in place for all types of transfer facilities within the organization and between the organization and other parties.

Implementation: your organization has established rules and procedures for the secure transfer of information. This includes the use of encryption for the transfer of sensitive information over public networks. We also have information transfer agreements in place with our partners and suppliers to ensure that they protect our information.

A.5.15 Access Control

Control: Access to information and other associated assets shall be restricted in accordance with the established topic-specific policy on access control.

Implementation: your organization has implemented a formal access control policy and procedures to restrict access to our information and other associated assets. Access is granted on the basis of the principle of least privilege, and all access is logged and monitored. The access control policy is reviewed and updated regularly.

A.5.16 Identity Management

Control: The full lifecycle of identities shall be managed.

Implementation: your organization has implemented an identity management system to manage the full lifecycle of user identities. This includes the creation, modification, and deletion of user accounts. The identity management system is integrated with our HR processes to ensure that user access is appropriate for their role.

A.5.17 Authentication Information

Control: Allocation and management of authentication information shall be controlled by a management process, including advising personnel on the appropriate handling of authentication information.

Implementation: your organization has a formal process for the allocation and management of authentication information, such as passwords and tokens. This process is documented in our password policy, which is communicated to all employees. The password policy includes requirements for password complexity, length, and history.

A.5.18 Access Rights

Control: Access rights to information and other associated assets shall be provisioned, reviewed, modified and removed in accordance with the organization's topic-specific policy on and rules for access control.

Implementation: your organization has a formal process for the provisioning, review, modification, and removal of access rights. This process is documented in our access control procedure. All access rights are reviewed on a regular basis to ensure that they are still required.

A.5.19 Information Security in Supplier Relationships

Control: Information security requirements for mitigating the risks associated with supplier's access to the organization's assets shall be agreed with the supplier and documented.

Implementation: Your organization has established a formal process for managing information security in supplier relationships. This process includes the identification of information security requirements for suppliers, the assessment of supplier security capabilities, and the monitoring of supplier compliance with security requirements. All suppliers are required to sign a supplier security agreement that defines their security obligations.

A.5.20 Addressing Information Security Within Supplier Agreements

Control: Relevant information security requirements shall be established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for, the organization's information.

Implementation: Your organization includes specific information security requirements in all supplier agreements. These requirements are tailored to the type of service being provided and the level of access the supplier will have to our information assets. The agreements

include provisions for security assessments, incident reporting, and the right to audit supplier security controls.

A.5.21 Managing Information Security in the ICT Supply Chain

Control: Processes and procedures shall be defined and implemented to manage the information security risks associated with the use of products or services from the ICT supply chain.

Implementation: Your organization has implemented a comprehensive ICT supply chain security management program. This includes the assessment of ICT suppliers, the monitoring of supply chain risks, and the implementation of controls to mitigate identified risks. We maintain an inventory of all ICT products and services in our supply chain and regularly assess their security posture.

A.5.22 Monitoring, Review and Change Management of Supplier Services

Control: The organization shall regularly monitor, review, audit and assess supplier service delivery.

Implementation: Your organization has established a formal process for monitoring, reviewing, and managing changes to supplier services. This includes regular performance reviews, security assessments, and the management of changes to supplier services. All supplier performance is monitored against agreed service levels and security requirements.

A.5.23 Information Security for Use of Cloud Services

Control: Processes for the acquisition, use, management and exit from cloud services shall be established in accordance with the organization's information security requirements.

Implementation: Your organization has developed a comprehensive cloud security strategy that covers the entire lifecycle of cloud service usage. This includes due diligence processes for cloud service selection, security requirements for cloud deployments, ongoing monitoring of cloud security posture, and secure exit procedures. All cloud services are assessed for compliance with our security requirements before deployment.

A.5.24 Information Security Incident Management Planning and Preparation

Control: The organization shall plan and prepare for managing information security incidents by defining, establishing and communicating information security incident management processes, roles and responsibilities.

Implementation: Your organization has established a comprehensive incident management program that includes incident response procedures, roles and responsibilities, communication plans, and escalation procedures. The incident management team is trained and equipped to respond to various types of security incidents.

Regular incident response exercises are conducted to test and improve our response capabilities.

A.5.25 Assessment and Decision on Information Security Events

Control: The organization shall assess information security events and decide if they are categorized as information security incidents.

Implementation: Your organization has implemented a formal process for assessing and categorizing information security events. This process includes criteria for determining whether an event constitutes a security incident, procedures for initial assessment, and escalation procedures for incidents that require immediate attention. All security events are logged and tracked through to resolution.

A.5.26 Response to Information Security Incidents

Control: Information security incidents shall be responded to in accordance with the documented procedures.

Implementation: Your organization has documented incident response procedures that define the steps to be taken when responding to different types of security incidents. These procedures include containment, eradication, recovery, and post-incident activities. The incident response team is trained to follow these procedures and has access to the necessary tools and resources.

A.5.27 Learning from Information Security Incidents

Control: Knowledge gained from analyzing and resolving information security incidents shall be used to reduce the likelihood or impact of future incidents.

Implementation: Your organization has implemented a formal process for learning from security incidents. This includes post-incident reviews, root cause analysis, and the identification of lessons learned. The knowledge gained from incidents is used to improve our security controls, procedures, and training programs. Incident trends are analyzed to identify systemic issues and areas for improvement.

A.5.28 Collection of Evidence

Control: The organization shall establish and implement procedures for the identification, collection, acquisition and preservation of information that can serve as evidence.

Implementation: Your organization has established formal procedures for the collection and preservation of digital evidence. These procedures are designed to ensure that evidence is collected in a forensically sound manner and can be used in legal proceedings if necessary. All personnel involved in evidence collection are trained in proper forensic procedures.

A.5.29 Information Security During Disruption

Control: The organization shall plan how to maintain information security at an appropriate level during disruption.

Implementation: Your organization has developed business continuity and disaster recovery plans that include provisions for maintaining information security during disruptions. These plans identify critical security controls that must be maintained during disruptions and provide alternative procedures for maintaining security when normal operations are not possible.

A.5.30 ICT Readiness for Business Continuity

Control: ICT readiness shall be planned, implemented, maintained and tested to ensure business continuity.

Implementation: Your organization has implemented comprehensive ICT business continuity planning that includes backup systems, redundant infrastructure, and recovery procedures. Regular testing is conducted to ensure that ICT systems can be recovered within acceptable timeframes. The business continuity plan is regularly reviewed and updated to reflect changes in our ICT environment.

A.5.31 Identification of Legal, Statutory, Regulatory and Contractual Requirements

Control: Legal, statutory, regulatory and contractual requirements relevant to information security and the organization's approach to meet these requirements shall be explicitly identified, documented and kept up to date.

Implementation: Your organization maintains a comprehensive register of all legal, statutory, regulatory, and contractual requirements that apply to our information security program. This register is regularly reviewed and updated to ensure that we remain compliant with all applicable requirements. Legal and compliance experts are consulted to ensure accurate interpretation of requirements.

A.5.32 Intellectual Property Rights

Control: The organization shall implement appropriate procedures to protect intellectual property rights.

Implementation: Your organization has implemented procedures to protect intellectual property rights, including both our own intellectual property and that of third parties. This includes controls for the use of licensed software, protection of proprietary information, and respect for third-party intellectual property rights. All employees are trained on intellectual property policies and procedures.

A.5.33 Protection of Records

Control: Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release.

Implementation: Your organization has implemented comprehensive records management procedures that ensure the protection of records throughout their lifecycle. This includes physical and logical access controls, backup and recovery procedures, and secure disposal methods. Records are classified according to their sensitivity and protected accordingly.

A.5.34 Privacy and Protection of PII

Control: The organization shall identify and meet requirements regarding the preservation of privacy and protection of PII according to applicable laws and regulations and contractual requirements.

Implementation: Your organization has implemented a comprehensive privacy program that includes policies and procedures for the collection, use, storage, and disposal of personally identifiable information (PII). This program is designed to comply with applicable privacy laws and regulations, including GDPR, CCPA, and other relevant privacy frameworks. Regular privacy impact assessments are conducted for new systems and processes.

A.5.35 Independent Review of Information Security

Control: The organization's approach to managing information security and its implementation shall be reviewed independently at planned intervals or when significant changes occur.

Implementation: Your organization conducts independent reviews of our information security program at planned intervals. These reviews are conducted by qualified internal or external auditors who are independent of the areas being reviewed. The reviews assess the effectiveness of our security controls and identify areas for improvement.

A.5.36 Compliance with Policies and Standards for Information Security

Control: Compliance with the organization's information security policies and standards shall be regularly reviewed.

Implementation: Your organization has implemented a formal compliance monitoring program that includes regular reviews of compliance with our information security

policies and standards. This includes automated monitoring where possible, as well as manual reviews and audits. Non-compliance issues are tracked and remediated in a timely manner.

A.5.37 Documented Operating Procedures

Control: Operating procedures for information processing facilities shall be documented and made available to users who need them.

Implementation: Your organization maintains comprehensive documented operating procedures for all information processing facilities. These procedures are regularly reviewed and updated to ensure they remain current and accurate. The procedures are made available to all users who need them through our document management system, and training is provided to ensure users understand and follow the procedures.

9.3 People Controls (A.6)

This section provides a summary of the people controls that have been implemented by your organization to manage information security.

A.6.1 Screening

Control: Background verification checks on all candidates for employment shall be carried out in accordance with relevant laws, regulations and ethics and shall be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.

Implementation: your organization conducts background verification checks on all candidates for employment. The extent of the checks is determined by the role and the level of access that the individual will have to our information assets. All checks are carried out in accordance with relevant laws and regulations.

A.6.2 Terms and Conditions of Employment

Control: The contractual agreements with employees and contractors shall state their and the organization's responsibilities for information security.

Implementation: All employees and contractors are required to sign a confidentiality agreement as part of their terms and conditions of employment. The agreement clearly states their responsibilities for protecting our information assets.

A.6.3 Information Security Awareness, Education and Training

Control: All employees of the organization and, where relevant, contractors, shall receive appropriate awareness of education and training and regular updates in organizational policies and procedures, as relevant for their job function.

Implementation: your organization has an ongoing security awareness program to ensure that all employees and contractors are aware of their information security responsibilities. The program includes regular training sessions, newsletters, and other forms of communication.

A.6.4 Disciplinary Process

Control: There shall be a formal and communicated disciplinary process to act against employees who have committed an information security breach.

Implementation: your organization has a formal disciplinary process for dealing with employees who have committed an information security breach. The process is documented in our employee handbook and is communicated to all employees.

A.6.5 Responsibilities After Termination or Change of Employment

Control: Information, security responsibilities and duties that remain valid after termination or change of employment shall be defined, enforced and communicated to all relevant employees and contractors.

Implementation: All employees and contractors are required to sign a confidentiality agreement that remains in effect after their employment or contract has been terminated. The agreement clearly states their ongoing responsibilities for protecting our information assets.

A.6.6 Confidentiality or Non-disclosure Agreements

Control: Confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified, regularly reviewed and documented.

Implementation: your organization uses confidentiality and non-disclosure agreements to protect our sensitive information. These agreements are reviewed and updated regularly to ensure that they are still relevant and effective.

A.6.7 Remote Working

Control: A topic-specific policy should be developed and implemented to protect information accessed, processed or stored at remote working sites.

Implementation: your organization has a remote working policy that defines the security requirements for employees who work from home or other remote locations. The policy includes requirements for secure access to our network, the use of encryption, and the physical security of remote working sites.

A.6.8 Information Security Event Reporting

Control: The organization shall provide a mechanism for employees to report observed or suspected information security events through appropriate channels in a timely manner.

Implementation: your organization has a formal process for reporting information security events. All employees are encouraged to report any observed or suspected security incidents to the Information Security Manager as soon as possible. The reporting process is documented in our incident management procedure.

9.4 Physical Controls (A.7)

This section provides a summary of the physical controls that have been implemented by your organization to manage information security.

A.7.1 Physical Security Perimeters

Control: Security perimeters shall be defined and used to protect areas that contain either sensitive or critical information and information processing facilities.

Implementation: your organization has established physical security perimeters to protect our facilities. Access to our facilities is controlled through the use of access cards and other physical security measures. All visitors are required to sign in and are escorted while on our premises.

A.7.2 Physical Entry Controls

Control: Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.

Implementation: your organization has implemented physical entry controls to protect our secure areas. This includes the use of access cards, biometric scanners, and other physical security measures. All access to secure areas is logged and monitored.

A.7.3 Securing Offices, Rooms and Facilities

Control: Physical security for offices, rooms and facilities shall be designed and applied.

Implementation: your organization has implemented physical security measures to protect our offices, rooms, and facilities. This includes the use of locks, alarms, and other physical security measures. All sensitive information is stored in locked cabinets or rooms.

A.7.4 Physical Security Monitoring

Control: Premises shall be continuously monitored for unauthorized physical access.

Implementation: your organization has implemented a physical security monitoring system to detect and respond to unauthorized physical access. This includes the use of CCTV cameras, intrusion detection systems, and other monitoring technologies. All security events are logged and investigated.

A.7.5 Protecting Against External and Environmental Threats

Control: Physical protection against natural disasters, malicious attack or accidents shall be designed and applied.

Implementation: your organization has implemented measures to protect our facilities from external and environmental threats. This includes the use of fire suppression systems, flood barriers, and other protective measures. We also have a disaster recovery plan in place to ensure that we can recover from a major incident.

A.7.6 Working in Secure Areas

Control: Procedures for working in secure areas shall be designed and applied.

Implementation: your organization has established procedures for working in secure areas. These procedures are designed to reduce the risk of unauthorized access to our information assets. All employees who work in secure areas are required to follow these procedures.

A.7.7 Clear Desk and Clear Screen

Control: A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities shall be adopted.

Implementation: your organization has a clear desk and clear screen policy to reduce the risk of unauthorized access to our information assets. All employees are required to lock their computers when they are away from their desks and to store all sensitive information in locked cabinets.

A.7.8 Equipment Siting and Protection

Control: Equipment shall be sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.

Implementation: your organization has implemented controls to protect our equipment from environmental threats and hazards. This includes the use of temperature and humidity controls, as well as physical security measures to prevent unauthorized access.

A.7.9 Security of Assets Off-Premises

Control: Assets off-premises shall be protected.

Implementation: your organization has a policy for the protection of assets that are used off-premises. This includes the use of encryption for laptops and other mobile devices, as well as procedures for the secure transport of assets.

A.7.10 Storage Media

Control: Storage media shall be managed through their lifecycle of procurement, use, transportation and disposal in accordance with the organization's classification scheme and handling requirements.

Implementation: your organization has a formal process for the management of storage media. This process is documented in our media handling procedure. All storage media is classified and handled according to the requirements of its classification level.

A.7.11 Supporting Utilities

Control: Information processing facilities shall be protected from power failures and other disruptions caused by failures in supporting utilities.

Implementation: your organization has implemented controls to protect our information processing facilities from power failures and other disruptions. This includes the use of uninterruptible power supplies (UPS) and backup generators.

A.7.12 Cabling Security

Control: Power and telecommunications cables carrying data or supporting information services shall be protected from interception, interference or damage.

Implementation: your organization has implemented controls to protect our cabling from interception, interference, or damage. This includes the use of cable trays and conduits, as well as physical security measures to prevent unauthorized access.

A.7.13 Equipment Maintenance

Control: Equipment shall be correctly maintained to ensure its continued availability and integrity.

Implementation: your organization has a formal process for the maintenance of our equipment. This process is documented in our equipment maintenance procedure. All maintenance is carried out by authorized personnel.

A.7.14 Secure Disposal or Re-use of Equipment

Control: All items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.

Implementation: your organization has a formal process for the secure disposal or re-use of equipment. This process is documented in our equipment disposal procedure. All sensitive data is securely overwritten or destroyed before equipment is disposed of or re-used.

9.5 Technological Controls (A.8)

This section provides a summary of the technological controls that have been implemented by your organization to manage information security.

A.8.1 Endpoint Device Protection

Control: Information on endpoint devices shall be protected.

Implementation: your organization has implemented endpoint protection on all of our devices. This includes the use of anti-malware software, firewalls, and other security measures. All devices are configured to meet our security standards.

A.8.2 Privileged Access Rights

Control: The allocation and use of privileged access rights shall be restricted and managed.

Implementation: your organization has a formal process for the allocation and use of privileged access rights. This process is documented in our privileged access management procedure. All privileged access is logged and monitored.

A.8.3 Information Access Restriction

Control: Access to information and other associated assets shall be restricted in accordance with the established topic-specific policy on access control.

Implementation: your organization has implemented a formal access control policy and procedures to restrict access to our information and other associated assets. Access is granted on the basis of the principle of least privilege, and all access is logged and monitored. The access control policy is reviewed and updated regularly.

A.8.4 Access to Source Code

Control: Access to source code, development tools and software libraries shall be restricted.

Implementation: your organization has implemented controls to restrict access to our source code. Access is granted on a need-to-know basis, and all access is logged and monitored. We also have a version control system in place to track all changes to our source code.

A.8.5 Secure Authentication

Control: Secure authentication technologies and procedures shall be implemented based on information access restrictions and the topic-specific policy on access control.

Implementation: your organization has implemented secure authentication technologies and procedures to protect our information assets. This includes the use of multi-factor authentication for all remote access to our network. We also have a password policy in place that requires the use of strong passwords.

A.8.6 Capacity Management

Control: The use of resources shall be monitored and tuned in line with current and expected capacity demands.

Implementation: your organization has a formal process for capacity management. This process is documented in our capacity management procedure. We monitor the use of our resources and plan for future capacity requirements.

A.8.7 Protection Against Malware

Control: Protection against malware shall be implemented and supported by appropriate user awareness.

Implementation: your organization has implemented anti-malware software on all of our devices. We also have a security awareness program in place to educate our employees about the risks of malware.

A.8.8 Management of Technical Vulnerabilities

Control: Information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.

Implementation: your organization has a formal process for the management of technical vulnerabilities. This process is documented in our vulnerability management procedure. We use a variety of tools to scan our systems for vulnerabilities, and we have a process in place for patching vulnerabilities in a timely manner.

A.8.9 Configuration Management

Control: Configurations, including security configurations, of hardware, software, services and networks shall be established, documented, implemented, monitored and reviewed.

Implementation: your organization has a formal process for configuration management. This process is documented in our configuration management procedure. We have a baseline configuration for all of our systems, and we have a process in place for managing changes to our configurations.

A.8.10 Information Deletion

Control: Information stored in information systems, devices or in any other storage media shall be deleted when no longer required.

Implementation: your organization has a formal process for the deletion of information. This process is documented in our data retention and deletion procedure. We have a data retention schedule that defines how long we keep different types of information, and we have a process in place for securely deleting information when it is no longer required.

A.8.11 Data Masking

Control: Data masking shall be used in accordance with the organization's topic-specific policy on access control and other related topic-specific policies, and business requirements, taking applicable legislation into consideration.

Implementation: your organization uses data masking to protect sensitive information.

This includes the use of data masking in our non-production environments. We have a formal process for data masking, which is documented in our data masking procedure.

A.8.12 Data Leakage Prevention

Control: Data leakage prevention measures shall be applied to systems, networks and any other devices that process, store or transmit sensitive information.

Implementation: your organization has implemented data leakage prevention measures to protect our sensitive information. This includes the use of data loss prevention (DLP) software, as well as other security measures. We have a formal process for data leakage prevention, which is documented in our data leakage prevention procedure.

A.8.13 Information Backup

Control: Backup copies of information, software and systems shall be taken and tested regularly in accordance with the agreed topic-specific policy on backup.

Implementation: your organization has a formal process for the backup of our information, software, and systems. This process is documented in our backup procedure. We have a backup schedule that defines how often we back up our data, and we have a process in place for testing our backups regularly.

A.8.14 Redundancy of Information Processing Facilities

Control: Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.

Implementation: your organization has implemented redundancy in our information processing facilities to meet our availability requirements. This includes the use of redundant servers, storage, and network equipment.

A.8.15 Logging

Control: Logs that record activities, exceptions, faults and other relevant events shall be produced, stored, protected and analyzed.

Implementation: your organization has implemented a logging system to record activities, exceptions, faults, and other relevant events. All logs are stored, protected, and analyzed in accordance with our logging procedure.

A.8.16 Monitoring Activities

Control: Networks, systems and applications shall be monitored for anomalous behavior and appropriate action taken to evaluate potential information security incidents.

Implementation: your organization has implemented a monitoring system to detect anomalous behavior on our networks, systems, and applications. All security events are logged and investigated in accordance with our incident management procedure.

A.8.17 Clock Synchronization

Control: The clocks of all relevant information processing systems within an organization or security domain shall be synchronized to a single reference time source.

Implementation: your organization has implemented a clock synchronization system to ensure that all of our systems have the same time. This is important for the analysis of security events.

A.8.18 Use of Privileged Utility Programs

Control: The use of utility programs that can override system and application controls shall be restricted and tightly controlled.

Implementation: your organization has a formal process for the use of privileged utility programs. This process is documented in our privileged access management procedure. All use of privileged utility programs is logged and monitored.

A.8.19 Installation of Software on Operational Systems

Control: Procedures and measures shall be implemented to securely manage software installation on operational systems.

Implementation: your organization has a formal process for the installation of software on our operational systems. This process is documented in our change management procedure. All software is tested and approved before it is installed on our operational systems.

A.8.20 Network Security

Control: Networks and network devices shall be secured, managed and controlled to protect information in systems and applications.

Implementation: your organization has implemented a variety of security measures to

protect our networks and network devices. This includes the use of firewalls, intrusion detection systems, and other security technologies. We have a formal process for network security, which is documented in our network security procedure.

A.8.21 Security of Network Services

Control: Security mechanisms, service levels and service requirements of network services shall be identified, implemented and monitored.

Implementation: your organization has a formal process for the security of our network services. This process is documented in our network security procedure. We have identified the security mechanisms, service levels, and service requirements for all of our network services.

A.8.22 Segregation of Networks

Control: Groups of information services, users and information systems shall be segregated on the organization's networks.

Implementation: your organization has implemented network segregation to protect our information assets. We have segregated our networks into different security zones, and we have implemented access controls to restrict traffic between the zones.

A.8.23 Web Filtering

Control: Access to external websites shall be managed to reduce exposure to malicious content.

Implementation: your organization has implemented a web filtering solution to protect our employees from malicious content. The web filtering solution blocks access to known malicious websites, and it also provides content filtering to prevent access to inappropriate websites.

A.8.24 Use of Cryptography

Control: Rules for the effective use of cryptography, including cryptographic key management, shall be defined and implemented.

Implementation: your organization has a formal process for the use of cryptography. This process is documented in our cryptography procedure. We use cryptography to protect our sensitive information, and we have a process in place for managing our cryptographic keys.

A.8.25 Secure Development Lifecycle

Control: Rules for the secure development of software and systems shall be established and applied.

Implementation: your organization has a formal process for the secure development of software and systems. This process is documented in our secure development lifecycle procedure. We have a set of security requirements that all of our software and systems must meet.

A.8.26 Application Security Requirements

Control: Information security requirements shall be identified, specified and approved when developing or acquiring applications.

Implementation: your organization has a formal process for identifying, specifying, and approving information security requirements for all of our applications. This process is documented in our application security requirements procedure.

A.8.27 Secure System Architecture and Engineering Principles

Control: Principles for engineering secure systems shall be established, documented, maintained and applied to any information system development activities.

Implementation: your organization has a set of secure system architecture and engineering principles that are applied to all of our information system development activities. These principles are documented in our secure system architecture and engineering principles procedure.

A.8.28 Secure Coding

Control: Secure coding principles shall be applied to software development.

Implementation: your organization has a set of secure coding principles that are applied to all of our software development. These principles are documented in our secure coding procedure. We also have a process in place for reviewing our code for security vulnerabilities.

A.8.29 Security Testing in Development and Acceptance

Control: Security testing processes shall be defined and implemented in the development lifecycle.

Implementation: your organization has a formal process for security testing in our development lifecycle. This process is documented in our security testing procedure. We

use a variety of tools to test our software for security vulnerabilities.

A.8.30 Outsourced Development

Control: The organization shall direct, monitor and review the activities related to outsourced system development.

Implementation: your organization has a formal process for managing outsourced development. This process is documented in our outsourced development procedure. We have a set of security requirements that all of our outsourced developers must meet.

A.8.31 Separation of Development, Testing and Production Environments

Control: Development, testing, and production environments shall be separated and secure.

Implementation: your organization has separated our development, testing, and production environments. We have implemented access controls to restrict access to each environment, and we have a process in place for managing changes to each environment.

A.8.32 Change Management

Control: Changes to information processing facilities and information systems shall be subject to a change in the management process.

Implementation: your organization has a formal process for change management. This process is documented in our change management procedure. All changes to our information processing facilities and information systems are reviewed and approved before they are implemented.

A.8.33 Test Information

Control: Test information shall be carefully selected, protected and managed.

Implementation: your organization has a formal process for the management of test information. This process is documented in our test data management procedure. We use a variety of techniques to protect our test information, such as data masking and anonymization.

A.8.34 Protection of Information Systems During Audit and Testing

Control: Audit tests and other assurance activities involving assessment of operational systems shall be planned and agreed to minimize the impact on business processes.

Implementation: your organization has a formal process for the protection of our information

systems during audit and testing. This process is documented in our audit and testing procedure. We work with our auditors to plan and agree on all audit tests and other assurance activities.

10. Appendices

This section contains supporting documentation for the ISMS.

10.1 Risk Assessment and Treatment Methodology

This document describes the methodology used by your organization to assess and treat information security risks. It includes the criteria for evaluating the likelihood and impact of risks, as well as the process for selecting and implementing controls.

10.1.1 Risk Identification

- Asset identification and classification
- Threat identification using industry threat intelligence sources
- Vulnerability assessment through automated scanning and manual reviews
- Risk scenario development based on threat-vulnerability combinations

10.1.2 Risk Analysis

- Likelihood assessment using a 5-point scale (Very Low, Low, Medium, High, Very High)
- Impact assessment considering confidentiality, integrity, and availability
- Risk calculation using the formula: Risk = Likelihood × Impact

10.1.3 Risk Evaluation

- Risk acceptance criteria: Low and Medium risks are generally acceptable
- High and Very High risks require treatment
- Risk tolerance levels defined by senior management

10.1.4 Risk Treatment Options

- **Avoid:** Eliminate the risk by removing the risk source
- **Reduce:** Implement controls to reduce likelihood or impact
- **Transfer:** Share risk through insurance or outsourcing
- **Accept:** Formally accept residual risk with management approval

10.1.5 Risk Treatment Plan

- Control selection from ISO 27001:2022 Annex A
- Implementation timeline and resource allocation
- Responsibility assignment for each control
- Monitoring and review procedures

10.1.6 Risk Assessment Frequency

- Annual comprehensive risk assessments
- Quarterly reviews of high-risk areas
- Ad-hoc assessments for significant changes
- Incident-driven assessments as required

10.2 List of Interested Parties

This document lists the interested parties of your organization and their requirements related to information security.

Interested Party	***Information Security Requirements***	***Communication Method***	***Review Frequency***
Customers	*-Data protection and privacy -Service availability (99.9% uptime) -incident Notification within 24 hours - compliance with Industry Standards*	*Customer portal, Email notifications*	*Quarterly*
Employees	*- Secure working environment- Clear security policies and procedures - Regular security training- Incident reporting mechanisms*	*-Internal communications, training sessions, intranet*	*Monthly*
Shareholders/ Investor s	*-Risk management and mitigation- Compliance with regulations- Financial impact assessment of security incidents - Business continuity assurance*	*Board meetings, annual reports, investor calls*	*Quarterly*
Regulatory Bodies	*- Compliance with GDPR, SOX, HIPAA (as applicable) - Audit trail maintenance - Incident reporting as required - Data localization requirements*	*Formal reports, audit submissions, regulatory filings*	*As required*
Suppliers/Vendors	*- Secure data exchange protocols - Vendor security assessments - Contractual security obligations - Supply chain security requirements*	*Vendor meetings, security assessments, contracts*	*Annually*
Business Partners	*- Secure collaboration platforms - Data sharing agreements - Joint incident response procedures - Mutual security standards*	*Partnership agreements, joint reviews, secure channels*	*Semi-Annually*
IT Service Providers	*- Infrastructure security standards- Monitoring and alerting requirements - Backup and recovery procedures - Change management processes*	*Service level agreements, technical meetings, reports*	*Monthly*
Legal/Compliance Team	*- Legal and regulatory compliance - Contract review and approval - Incident legal implications - Intellectual property protection*	*Legal reviews, compliance reports, policy updates*	*As Needed*
Insurance Providers	*- Risk assessment documentation- Security control implementation - Incident reporting and claims-*	*Insurance assessments, claims reports, annual*	*Annually*

	Premium calculation factors	*reviews*	
Local Community	*- Environmental impact of security measures - Emergency response coordination - Public safety considerations - Community Notification procedures*	*Public notices, emergency services coordination*	*As Needed*

10.3 Communication Plan

This document describes the communication plan for the ISMS. It includes what, when, to whom, and how communication related to information security.

ISMS Communication plan

1. Communication Objectives

- Ensure all stakeholders are informed about ISMS policies, procedures, and requirements
- Promote security awareness and culture throughout the organization
- Facilitate effective incident communication and response
- Maintain transparency with external stakeholders regarding security posture

2. Internal Communication

Target Audience	***Communication Type***	***Content***	***Frequency***	***Method***	***Responsible Party***
All Employee	*Security Awareness, Policy Update, Training*	*Monthly security tips, threat updates, policy reminders*	*Monthly*	*Email newsletter, intranet*	*CISO Office, HR*
Management Team	*ISMS Performance*	*KPI reports, risk assessments, audit results*	*Monthly*	*Management meetings, dashboards*	*CISO*
IT Staff	*Technical Updates*	*Incident status, response actions, lessons learned*	*During incidents*	*Secure communication channels*	*IT Security Team*
Incident Response Team	*Incident Communications*	*Incident status, response actions,*	*During incidents*	*Board Presentations, Report*	*Incident Officer*

		lessons learned			
Board of Directors	*Strategic Updates*	*ISMS effectiveness, major risks, compliance status*	*Quarterly*	*Board Presentations, Report*	*CISO*

2. External Communication

Target Audience	***Communication Type***	***Content***	***Frequency***	***Method***	***Responsible Party***
Customers	*Security posture*	*Certification status, security measures, incident notifications*	*Quarterly/As needed*	*Customer portal, newsletters*	*Customer Relations*
Regulatory	*Compliance Report*	*Audit results, incident reports, compliance status*	*As Required*	*Formal Submission*	*Legal/Compliance*
Suppliers	*Security Requirements*	*Security standards, assessment results, contract requirements*	*Annually*	*Vendor meetings, contracts*	*Procurement*
Partners	*Collaboration Security*	*Joint security measures, shared responsibilities, incident coordination*	*Semi-Annually*	*Partnership meetings*	*Business Development*
Public/Media	*Incident Communication*	*Public incident notifications, security initiatives*	*As Needed*	*Press releases, Website*	*Communications Teams*

3. Incident Communication Procedure

3.1 Internal Incident Communication

- Immediate notification to Incident Response Team (within 15 minutes)
- Management notification for high-severity incidents (within 1 hour)
- Regular status updates during incident response (every 2 hours)
- Post-incident communication and lessons learned (within 48 hours)

3.2 External Incident Communication

- Customer notification for incidents affecting their data (within 24 hours)
- Regulatory notification as required by law (within 72 hours for GDPR)
- Partner notification for incidents affecting shared systems (within 4 hours)
- Public communication for significant incidents (as determined by management)

4. Communication Channels and Tools

Channel	***Purpose***	***Security Level***	***Access Control***
Corporate Email	*General communications, policy updates*	*Standard*	*All employees*
Secure Messaging Platform	*Sensitive communications, incident response*	*Encrypted*	*Authorized personnel*
Intranet Portal	*Policy repository, training materials*	*Internal*	*All employees*
Customer Portal	*Customer-facing security information*	*Controlled*	*Customers only*
Emergency Notification System	*Critical incident alerts*	*High priority*	*Emergency contacts*
Video Conferencing	*Training sessions, management meetings*	*Standard*	*Meeting participants*

5. Communication Effectiveness Measurement

- Employee security awareness survey (annually)
- Communication reach and engagement metrics (monthly)
- Incident communication response times (per incident)
- Stakeholder feedback on communication effectiveness (quarterly)
- Training completion rates and assessment scores (quarterly)

10.4 Other relevant documents and records

This section contains other relevant documents and records that support the ISMS, such as:

- Information Security Policy
- Statement of Applicability (SoA)
- Risk Assessment Report
- Risk Treatment Plan
- Internal Audit Reports
- Management Review Minutes

[Placeholder for other relevant documents and records]