ISO 27002 - 2022

Policies and Procedures

CONFIDENTIALITY NOTE: The information contained in this report document is for the exclusive use of the client specified above and may contain confidential, privileged and non-disclosable information. If the recipient of this report is not the client or addressee, such recipient is strictly prohibited from reading, photocopying, distributing or otherwise using this report or its contents in any way.

Prepared for: Client Company

Prepared by: YourIT Company

Table of Contents

Purpose

The purpose is to ensure the security of data aligned with an internationally recognized Information Management Security System (ISMS) standard for cybersecurity, to meet regulatory, contractual, or insurance requirements, or to ensure a high level of data protection.

Scope

This policy applies to the workforce members and vendors of the organization that come in contact with sensitive, confidential, and/or protected data.

Sanctions/Compliance

Failure to comply with this or any other security policy will result in disciplinary actions as per the Sanction Policy. Legal actions also may be taken for violations of applicable regulations and laws.

ISO 27002:2022-(5) - Organizational Controls

ISO 27002 - 2022	**Other Requirements**
ISO 27002:2022-(5) Organizational Controls	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

Controls:

5.1 - Policies for information security
5.2 - Information security roles and responsibilities
5.3 - Segregation of duties
5.4 - Management responsibilities
5.5 - Contact with authorities
5.6 - Contact with special interest groups
5.7 - Threat intelligence
5.8 - Information security in project management
5.9 - Inventory of information and other associated assets
5.10 - Acceptable use of information and other associated assets
5.11 - Return of assets
5.12 - Classification of information
5.13 - Labelling of information
5.14 - Information transfer
5.15 - Access control
5.16 - Identity management
5.17 - Authentication information
5.18 - Access rights
5.19 - Information security in supplier relationships
5.20 - Addressing information security within supplier agreements
5.21 - Managing information security in the ICT supply chain
5.22 - Monitoring, review and change management of supplier services
5.23 - Information security for use of cloud services
5.24 - Information security incident management planning and preparation
5.25 - Assessment and decision on information security events
5.26 - Response to information security incidents
5.27 - Learning from information security incidents
5.28 - Collection of evidence
5.29 - Information security during disruption
5.30 - ICT readiness for business continuity
5.31 - Legal, statutory, regulatory and contractual requirements
5.32 - Intellectual property rights
5.33 - Protection of records
5.34 - Privacy and protection of PII
5.35 - Independent review of information security
5.36 - Compliance with policies, rules and standards for information security
5.37 - Documented operating procedures

Guidance
Organizational controls include rules and measures that regulate and control an organization's comprehensive approach to data protection across a wide range of matters that lie beyond the scope of the People, Physical, and Technological Controls. These controls include policies, rules, processes, procedures, organizational structures, etc.

Number of controls: 37

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls

- ISO 27002:2022-(5.1) - Policies for information security:

  Control
  Information security policy and topic-specific policies should be defined, approved by management, published, communicated to and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur.

  Purpose
  To ensure continuing suitability, adequacy, effectiveness of management direction and support for information security in accordance with business, legal, statutory, regulatory and contractual requirements.

- ISO 27002:2022-(5.2) - Information security roles and responsibilities:

  Control
  Information security roles and responsibilities should be defined and allocated according to the organization needs.

  Purpose
  To establish a defined, approved and understood structure for the implementation, operation and management of information security within the organization.

- ISO 27002:2022-(5.3) - Segregation of duties:

  Control
  Conflicting duties and conflicting areas of responsibility should be segregated.

  Purpose
  To reduce the risk of fraud, error and bypassing of information security controls.

- ISO 27002:2022-(5.4) - Management responsibilities:

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

  Purpose
  To ensure management understand their role in information security and undertake actions aiming to ensure all personnel are aware of and fulfil their information security responsibilities.

- ISO 27002:2022-(5.5) - Contact with authorities:

  Control
  The organization should establish and maintain contact with relevant authorities.

  Purpose
  To ensure appropriate flow of information takes place with respect to information security between the organization and relevant legal, regulatory and supervisory authorities.

- ISO 27002:2022-(5.6) - Contact with special interest groups:

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

  Purpose
  To ensure appropriate flow of information takes place with respect to information security.

- ISO 27002:2022-(5.7) - Threat intelligence:

  Control
  Information relating to information security threats should be collected and analysed to produce threat intelligence.

  Purpose
  To provide awareness of the organization’s threat environment so that the appropriate mitigation actions can be taken.

- ISO 27002:2022-(5.8) - Information security in project management:

  Control
  Information security should be integrated into project management.

  Purpose
  To ensure information security risks related to projects and deliverables are effectively addressed in project management throughout the project life cycle.

- ISO 27002:2022-(5.9) - Inventory of information and other associated assets:

  Control
  An inventory of information and other associated assets, including owners, should be developed and maintained.

  Purpose
  To identify the organization’s information and other associated assets in order to preserve their information security and assign appropriate ownership.

- ISO 27002:2022-(5.10) - Acceptable use of information and other associated assets:

  Control
  Rules for the acceptable use and procedures for handling information and other associated assets should be identified, documented and implemented.

  Purpose
  To ensure information and other associated assets are appropriately protected, used and handled.

- ISO 27002:2022-(5.11) - Return of assets:

  Control
  Personnel and other interested parties as appropriate should return all the organization’s assets in their possession upon change or termination of their employment, contract or agreement.

  Purpose
  To protect the organization’s assets as part of the process of changing or terminating employment, contract or agreement.

- ISO 27002:2022-(5.12) - Classification of information:

  Control

Information should be classified according to the information security needs of the organization based on confidentiality, integrity, availability and relevant interested party requirements.

Purpose
To ensure identification and understanding of protection needs of information in accordance with its importance to the organization.

- ISO 27002:2022-(5.13) - Labelling of information:
  Control
  An appropriate set of procedures for information labelling should be developed and implemented in accordance with the information classification scheme adopted by the organization.

  Purpose
  To facilitate the communication of classification of information and support automation of information processing and management.

- ISO 27002:2022-(5.14) - Information transfer:
  Control
  Information transfer rules, procedures, or agreements should be in place for all types of transfer facilities within the organization and between the organization and other parties.

  Purpose
  To maintain the security of information transferred within an organization and with any external interested party.

- ISO 27002:2022-(5.15) - Access control:
  Control
  Rules to control physical and logical access to information and other associated assets should be established and implemented based on business and information security requirements.

  Purpose
  To ensure authorized access and to prevent unauthorized access to information and other associated assets.

- ISO 27002:2022-(5.16) - Identity management:
  Control
  The full life cycle of identities should be managed.

  Purpose
  To allow for the unique identification of individuals and systems accessing the organization's information and other associated assets and to enable appropriate assignment of access rights.

- ISO 27002:2022-(5.17) - Authentication information:
  Control
  Allocation and management of authentication information should be controlled by a management process, including advising personnel on the appropriate handling of authentication information.

  Purpose
  To ensure proper entity authentication and prevent failures of authentication processes.

- ISO 27002:2022-(5.18) - Access rights:
  Control

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

Purpose
To ensure access to information and other associated assets is defined and authorized according to the business requirements.

- ISO 27002:2022-(5.19) - Information security in supplier relationships:
  Control
  Processes and procedures should be defined and implemented to manage the information security risks associated with the use of supplier’s products or services.

  Purpose
  To maintain an agreed level of information security in supplier relationships.

- ISO 27002:2022-(5.20) - Addressing information security within supplier agreements:
  Control
  Relevant information security requirements should be established and agreed with each supplier based on the type of supplier relationship.

  Purpose
  To maintain an agreed level of information security in supplier relationships.

- ISO 27002:2022-(5.21) - Managing information security in the ICT supply chain:
  Control
  Processes and procedures should be defined and implemented to manage the information security risks associated with the ICT products and services supply chain.

  Purpose
  To maintain an agreed level of information security in supplier relationships.

- ISO 27002:2022-(5.22) - Monitoring, review and change management of supplier services:
  Control
  The organization should regularly monitor, review, evaluate and manage change in supplier information security practices and service delivery.

  Purpose
  To maintain an agreed level of information security and service delivery in line with supplier agreements.

- ISO 27002:2022-(5.23) - Information security for use of cloud services:
  Control
  Processes for acquisition, use, management and exit from cloud services should be established in accordance with the organization’s information security requirements.

  Purpose
  To specify and manage information security for the use of cloud services.

- ISO 27002:2022-(5.24) - Information security incident management planning and preparation:
  Control
  The organization should plan and prepare for managing information security incidents by defining, establishing and communicating information security incident management processes, roles and responsibilities.

  Purpose
  To ensure quick, effective, consistent and orderly response to information security incidents, including communication on information security events.

- ISO 27002:2022-(5.25) - Assessment and decision on information security events:

  Control
  The organization should assess information security events and decide if they are to be categorized as information security incidents.

  Purpose
  To ensure effective categorization and prioritization of information security events.

- ISO 27002:2022-(5.26) - Response to information security incidents:

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

  Purpose
  To ensure efficient and effective response to information security incidents.

- ISO 27002:2022-(5.27) - Learning from information security incidents:

  Control
  Knowledge gained from information security incidents should be used to strengthen and improve the information security controls.

  Purpose
  To reduce the likelihood or consequences of future incidents.

- ISO 27002:2022-(5.28) - Collection of evidence:

  Control
  The organization should establish and implement procedures for the identification, collection, acquisition and preservation of evidence related to information security events.

  Purpose
  To ensure a consistent and effective management of evidence related to information security incidents for the purposes of disciplinary and legal actions.

- ISO 27002:2022-(5.29) - Information security during disruption:

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

  Purpose
  To protect information and other associated assets during disruption.

- ISO 27002:2022-(5.30) - ICT readiness for business continuity:

  Control
  ICT readiness should be planned, implemented, maintained and tested based on business continuity objectives and ICT continuity requirements.

  Purpose
  To ensure the availability of the organization’s information and other associated assets during disruption.

- ISO 27002:2022-(5.31) - 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 should be identified, documented and kept up to date.

  Purpose

To ensure compliance with legal, statutory, regulatory and contractual requirements related to information security.

- ISO 27002:2022-(5.32) - Intellectual property rights:

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

  Purpose
  To ensure compliance with legal, statutory, regulatory and contractual requirements related to intellectual property rights and use of proprietary products.

- ISO 27002:2022-(5.33) - Protection of records:

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

  Purpose
  To ensure compliance with legal, statutory, regulatory and contractual requirements, as well as community or societal expectations related to the protection and availability of records.

- ISO 27002:2022-(5.34) - Privacy and protection of PII:

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

  Purpose
  To ensure compliance with legal, statutory, regulatory and contractual requirements related to the information security aspects of the protection of PII.

- ISO 27002:2022-(5.35) - Independent review of information security:

  Control
  The organization's approach to managing information security and its implementation including people, processes and technologies should be reviewed independently at planned intervals, or when significant changes occur.

  Purpose
  To ensure the continuing suitability, adequacy and effectiveness of the organization's approach to managing information security.

- ISO 27002:2022-(5.36) - Compliance with policies, rules and standards for information security:

  Control
  Compliance with the organization's information security policy, topic-specific policies, rules and standards should be regularly reviewed.

  Purpose
  To ensure that information security is implemented and operated in accordance with the organization's information security policy, topic-specific policies, rules and standards.

- ISO 27002:2022-(5.37) - Documented operating procedures:

  Control
  Operating procedures for information processing facilities should be documented and made available to personnel who need them.

  Purpose

To ensure the correct and secure operation of information processing facilities.

References

- ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection Information security controls - https://www.iso.org/standard/75652.html

ISO 27002:2022-(6) - People Controls

ISO 27002 - 2022 ISO 27002:2022-(6) People Controls	**Other Requirements** N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

Controls:

6.1 - Screening
6.2 - Terms and conditions of employment
6.3 - Information security awareness, education and training
6.4 - Disciplinary process
6.5 - Responsibilities after termination or change of employment
6.6 - Confidentiality or non-disclosure agreements
6.7 - Remote working
6.8 - Information security event reporting

Guidance
People controls allow organizations to regulate the people component of their information security program by defining how employees and other workforce members interact with data and each other. These controls include secure HR onboarding, offboarding, personnel security, remote working, and security awareness education and training.

Number of controls: 8

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls

- ISO 27002:2022-(6.1) - Screening:

  Control
  Background verification checks on all candidates to become personnel should be carried out prior to joining the organization and on an ongoing basis taking into consideration applicable laws, regulations and ethics and be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.

  Purpose
  To ensure all personnel are eligible and suitable for the roles for which they are considered and remain eligible and suitable during their employment.

- ISO 27002:2022-(6.2) - Terms and conditions of employment:

  Control
  The employment contractual agreements should state the personnel’s and the organization’s responsibilities for information security.

  Purpose
  To ensure personnel understand their information security responsibilities for the roles for which they are considered.

- ISO 27002:2022-(6.3) - Information security awareness, education and training:

  Control
  Personnel of the organization and relevant interested parties should receive appropriate information security awareness, education and training and regular updates of the organization's information security policy, topic-specific policies and procedures, as relevant for their job function.

  Purpose
  To ensure personnel and relevant interested parties are aware of and fulfil their information security responsibilities.

- ISO 27002:2022-(6.4) - Disciplinary process:

  Control
  A disciplinary process should be formalized and communicated to take actions against personnel and other relevant interested parties who have committed an information security policy violation.

  Purpose
  To ensure personnel and other relevant interested parties understand the consequences of information security policy violation, to deter and appropriately deal with personnel and other relevant interested parties who committed the violation.

- ISO 27002:2022-(6.5) - Responsibilities after termination or change of employment:

  Control
  Information security responsibilities and duties that remain valid after termination or change of employment should be defined, enforced and communicated to relevant personnel and other interested parties.

  Purpose
  To protect the organization’s interests as part of the process of changing or terminating employment or contracts.

- ISO 27002:2022-(6.6) - Confidentiality or non-disclosure agreements:

  Control
  Confidentiality or non-disclosure agreements reflecting the organization’s needs for the protection of information should be identified, documented, regularly reviewed and signed by personnel and other relevant interested parties.

  Purpose
  To maintain confidentiality of information accessible by personnel or external parties.

- ISO 27002:2022-(6.7) - Remote working:

  Control
  Security measures should be implemented when personnel are working remotely to protect information accessed, processed or stored outside the organization’s premises.

  Purpose
  To ensure the security of information when personnel are working remotely.

- ISO 27002:2022-(6.8) - Information security event reporting:

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

  Purpose
  To support timely, consistent and effective reporting of information security events that can be identified by personnel.

References

- ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection Information security controls - https://www.iso.org/standard/75652.html

ISO 27002:2022-(7) - Physical Controls

ISO 27002 - 2022	**Other Requirements**
ISO 27002:2022-(7) Physical Controls	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

Controls:

7.1 - Physical security perimeters
7.2 - Physical entry
7.3 - Securing offices, rooms and facilities
7.4 - Physical security monitoring
7.5 - Protecting against physical and environmental threats
7.6 - Working in secure areas
7.7 - Clear desk and clear screen
7.8 - Equipment siting and protection
7.9 - Security of assets off-premises
7.10 - Storage media
7.11 - Supporting utilities
7.12 - Cabling security
7.13 - Equipment maintenance
7.14 - Secure disposal or re-use of equipment

Guidance
Physical controls are protection measures to ensure the safety of physical assets. This may include access to facilities and systems, visitor access, equipment disposal procedures, storage media protocols and clear desk policies. These controls are critical to protecting confidential information and its integrity.

Number of controls: 14

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls

- ISO 27002:2022-(7.1) - Physical security perimeters:

  Control
  Security perimeters should be defined and used to protect areas that contain information and other associated assets.

  Purpose
  To prevent unauthorized physical access, damage and interference to the organization’s information and other associated assets.

- ISO 27002:2022-(7.2) - Physical entry:

  Control

Secure areas should be protected by appropriate entry controls and access points.

Purpose
To ensure only authorized physical access to the organization’s information and other associated assets occurs.

- ISO 27002:2022-(7.3) - Securing offices, rooms and facilities:
  Control
  Physical security for offices, rooms and facilities should be designed and implemented.

  Purpose
  To prevent unauthorized physical access, damage and interference to the organization’s information and other associated assets in offices, rooms and facilities.

- ISO 27002:2022-(7.4) - Physical security monitoring:
  Control
  Premises should be continuously monitored for unauthorized physical access.

  Purpose
  To detect and deter unauthorized physical access.

- ISO 27002:2022-(7.5) - Protecting against physical and environmental threats:
  Control
  Protection against physical and environmental threats, such as natural disasters and other intentional or unintentional physical threats to infrastructure should be designed and implemented.

  Purpose
  To prevent or reduce the consequences of events originating from physical and environmental threats.

- ISO 27002:2022-(7.6) - Working in secure areas:
  Control
  Security measures for working in secure areas should be designed and implemented.

  Purpose
  To protect information and other associated assets in secure areas from damage and unauthorized interference by personnel working in these areas.
  ?

- ISO 27002:2022-(7.7) - Clear desk and clear screen:
  Control
  Clear desk rules for papers and removable storage media and clear screen rules for information processing facilities should be defined and appropriately enforced.

  Purpose
  To reduce the risks of unauthorized access, loss of and damage to information on desks, screens and in other accessible locations during and outside normal working hours.

- ISO 27002:2022-(7.8) - Equipment siting and protection:
  Control
  Equipment should be sited securely and protected.

  Purpose
  To reduce the risks from physical and environmental threats, and from unauthorized access and damage.

- ISO 27002:2022-(7.9) - Security of assets off-premises:

Control
Off-site assets should be protected.

Purpose
To prevent loss, damage, theft or compromise of off-site devices and interruption to the organization’s operations.

- ISO 27002:2022-(7.10) - Storage media:
  Control
  Storage media should be managed through their life cycle of acquisition, use, transportation and disposal in accordance with the organization’s classification scheme and handling requirements.

  Purpose
  To ensure only authorized disclosure, modification, removal or destruction of information on storage media.

- ISO 27002:2022-(7.11) - Supporting utilities:
  Control
  Information processing facilities should be protected from power failures and other disruptions caused by failures in supporting utilities.

  Purpose
  To prevent loss, damage or compromise of information and other associated assets, or interruption to the organization’s operations due to failure and disruption of supporting utilities.

- ISO 27002:2022-(7.12) - Cabling security:
  Control
  Cables carrying power, data or supporting information services should be protected from interception, interference or damage.

  Purpose
  To prevent loss, damage, theft or compromise of information and other associated assets and interruption to the organization’s operations related to power and communications cabling.

- ISO 27002:2022-(7.13) - Equipment maintenance:
  Control
  Equipment should be maintained correctly to ensure availability, integrity and confidentiality of information.

  Purpose
  To prevent loss, damage, theft or compromise of information and other associated assets and interruption to the organization’s operations caused by lack of maintenance.

- ISO 27002:2022-(7.14) - Secure disposal or re-use of equipment:
  Control
  Items of equipment containing storage media should be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.

  Purpose
  To prevent leakage of information from equipment to be disposed or re-used.

References

- ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection Information security controls - https://www.iso.org/standard/75652.html

ISO 27002:2022-(8) - Technological Controls

ISO 27002 - 2022 ISO 27002:2022-(8) Technological Controls	**Other Requirements** N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

Controls:

8.1 - User endpoint devices
8.2 - Privileged access rights
8.3 - Information access restriction
8.4 - Access to source code
8.5 - Secure authentication
8.6 - Capacity management
8.7 - Protection against malware
8.8 - Management of technical vulnerabilities
8.9 - Configuration management
8.10 - Information deletion
8.11 - Data masking
8.12 - Data leakage prevention
8.13 - Information backup
8.14 - Redundancy of information processing facilities
8.15 - Logging
8.16 - Monitoring activities
8.17 - Clock synchronization
8.18 - Use of privileged utility programs
8.19 - Installation of software on operational systems
8.20 - Networks security
8.21 - Security of network services
8.22 - Segregation of networks
8.23 - Web filtering
8.24 - Use of cryptography
8.25 - Secure development life cycle
8.26 - Application security requirements
8.27 - Secure system architecture and engineering principles
8.28 - Secure coding
8.29 - Security testing in development and acceptance
8.30 - Outsourced development
8.31 - Separation of development, test and production environments
8.32 - Change management
8.33 - Test information
8.34 - Protection of information systems during audit testing

Guidance

Technological controls specify the IT security practices that organizations should implement to establish a secure IT infrastructure, from access control to information system security, backup and data recovery strategies, audit logging, and monitoring.

Number of controls: 34

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls

- ISO 27002:2022-(8.1) - User endpoint devices:

  Control
  Information stored on, processed by or accessible via user endpoint devices should be protected.

  Purpose
  To protect information against the risks introduced by using user endpoint devices.

- ISO 27002:2022-(8.2) - Privileged access rights:

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

  Purpose
  To ensure only authorized users, software components and services are provided with privileged access rights.

- ISO 27002:2022-(8.3) - Information access restriction:

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

  Purpose
  To ensure only authorized access and to prevent unauthorized access to information and other associated assets.

- ISO 27002:2022-(8.4) - Access to source code:

  Control
  Read and write access to source code, development tools and software libraries should be appropriately managed.

  Purpose
  To prevent the introduction of unauthorized functionality, avoid unintentional or malicious changes and to maintain the confidentiality of valuable intellectual property.

- ISO 27002:2022-(8.5) - Secure authentication:

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

  Purpose
  To ensure a user or an entity is securely authenticated, when access to systems, applications and services is granted.

- ISO 27002:2022-(8.6) - Capacity management:

  Control
  The use of resources should be monitored and adjusted in line with current and expected capacity requirements.

Purpose
To ensure the required capacity of information processing facilities, human resources, offices and other facilities.

Truncated Sample Document