# Princess Sumaya University for Technology

King Abdullah II Faculty of Engineering

Computer Engineering Department

Princess Sumaya جامعـــة
University الأميـــرة سميّـــة
for Technology للتكنولوجيا

## IT SECURITY MANAGEMENT ISMS PROJECT


*Author:*

Anas Ereiqat 20200231

*Supervisor:*

Dr. Ali Alhaj


*Jan 22, 2024*

# TABLE OF CONTENTS

# 1 INTRODUCTION

Founded in 2018, CyberGuard Innovations Ltd. is a private company in AL-Abdali that's all about cybersecurity. They're really good at using the latest technology to keep things safe. They care a lot about keeping client info private. All the staff info and important data are stored in their local servers. Since technology is super important for CyberGuard, they make sure everything in their system stays safe. This is a big deal because it helps the company keep running smoothly and keeps its good reputation in the cybersecurity world.

## 1.1 OBJECTIVES

The primary goal of this project is to enhance the cybersecurity measures at CyberGuard Innovations Ltd. We plan to achieve this by conducting a comprehensive risk assessment of all company assets. The assessment will strictly comply to the ISO 27001 standard, guiding us through a detailed review of the statement of applicability. Subsequently, we will implement the necessary controls prescribed by the standard to fortify our cybersecurity framework and ensure the integrity and security of our systems and data.

# 2 CyberGuard ASSETS

This section will identify the list of assets of different types in the company.

## 2.1 HARDWARE ASSETS

The table below lists all the hardware assets included in the hospital's scope.

| # | Hardware Type | Vulnerabilities |
|---|---|---|
| **1** | High-Performance Computing Infrastructure | Overheating, Power Outages, Hardware Failures. |
| **2** | Network Devices (Routers, Switches) | Unauthorized Access, Firmware Vulnerabilities, DDoS Attacks. |
| **3** | Servers (Local and Cloud-based) | Software Exploits, Unauthorized Access, Data Breaches |
| **4** | Workstations and Laptops | Malware Infections, Phishing Attacks, Physical Theft. |

| | | |
|---|---|---|
| **5** | Mobile Devices (Smartphones, Tablets) | Data Leakage, Malicious Apps, Device Loss or Theft |
| **6** | Data Storage Devices (Hard Drives, SSDs) | Data Corruption, Data Theft, Physical Damage |
| **7** | Physical Security Systems (CCTV, Access Control) | Tampering, Unauthorized Access, Communication Interception |

## 2.2 Software Assets

The table below lists all the software assets included in the hospital's scope.

| # | Software Type | Vulnerabilities |
|---|---|---|
| 1 | Operating Systems | Unpatched Vulnerabilities, Malware Exploits, Insider Threats |
| 2 | Security Software (Firewalls, Antivirus) | Inadequate Configuration, Signature Lag, False Positives |
| 3 | Database Management Systems (DBMS) | SQL Injection, Insecure Configurations, Unauthorized Access |
| 4 | Web Applications | Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), Session Hijacking |
| 5 | Encryption Software | Weak Encryption Algorithms, Key Management Issues, Implementation Flaws |
| 6 | Authentication Systems | Weak Password Policies, Credential Stuffing, Brute Force Attacks |
| 7 | Network Monitoring Tools | Misconfigurations, Lack of Real-time Alerts, Data Overload |
| 8 | Collaboration Software (Messaging, Video Conferencing) | Data Leakage, Unauthorized Access, Endpoint Vulnerabilities |
| 9 | Backup and Recovery Software | Insufficient Backup Frequency, Lack of Encryption, Data Integrity Concerns |
| 10 | Patch Management Tools | Delayed Patch Deployments, Incomplete Vulnerability Assessment, Compatibility Issues |

### 2.3 Information Assets

The table below lists all the information assets included in the hospital's scope.

| # | **Information Assets** | **Vulnerabilities** |
|---|---|---|
| 1 | Proprietary Threat Intelligence Databases | Unauthorized Access, Data Corruption, Insider Threats |
| 2 | Client Confidentiality (Sensitive Cybersecurity Strategies) | Data Breaches, Insider Threats, Unauthorized Access |
| 3 | Research and Development Prototypes | Intellectual Property Theft, Unauthorized Access |

### 2.4 Business Assets

The table below lists all the business assets included in the hospital's scope.

| # | **Business Type** | **Vulnerabilities** |
|---|---|---|
| **1** | Customer Base | Loss of Customers, Negative Feedback, Data Breaches |
| **2** | Staff and Employee Information | Unauthorized Access, Data Breaches, Insider Threats |
| **3** | Brand Reputation | Negative Publicity, Social Media Attacks, Customer Complaints |

# 3 Enterprise Policy

### 3.1 Purpose

This policy is here to explain the rules that keep our company's information safe. We want to make sure data is private, accurate, and available when needed.

## 3.2 Scope

These rules apply to everyone in our company – employees, contractors, vendors, guests, and anyone connected to us. The rules cover everything we use, like computers, systems, and our physical spaces.

## 3.3 Information Security Policy

### 3.3.1 Principle

Our main rule is to have clear steps to protect patient privacy and make sure information stays safe and available.

### 3.3.2 Chief Executives Statement of Commitment

Our leaders promise to focus on risk, make sure everyone understands risks, and follow rules to keep data safe.

### 3.3.3 Introduction

Keeping information safe is really important for our employees, customers, and the company. We use a system to manage information security to keep things running smoothly.

### 3.3.4 Information Security Defined

Information security means making sure information is private, accurate, and always available.

| | |
|---|---|
| Confidentiality | Information is private and hidden. |
| Integrity | Information is complete and accurate. |
| Availability | Information and services are available and ready for use. |

### 3.3.5 Information Security Objectives: What We Want to Achieve

We want to have what we need to keep information safe and protect the data we collect. Our goal is to make sure our company keeps working well.

### 3.3.6 Information Security Policy Framework

The information security management system is built upon an information security policy framework. In conjunction with this policy, the following policies make up the policy framework:

- P1: Acceptable Encryption Policy.
- P2: Acceptable Use Policy.
- P3: Backup Policy.
- P4: Clean Desk Policy.
- P5: Data Breach Response Policy.
- P6: Email Retention Policy.
- P7: Employee Internet Use Monitoring and Filtering Policy.
- P8: End User Encryption Key Protection Policy.
- P9: Internet Usage Policy.
- P10: Lab Security Policy.
- P11: Password Construction Guidelines.
- P12: Password Protection Policy.
- P13: Remote Access Policy.
- P14: Removable Media Policy.
- P15: Risk Assessment Policy.
- P16: Security Response Plan Policy.
- P17: Software Installation Policy.

The documents for each policy can be found in the folder titled “All Policies” uploaded to the Drive.

### 3.3.7 Information Security Roles and Responsibilities

Everyone has a role in keeping information safe, from the top leaders to each team member. We all need to follow the rules and report anything that seems suspicious.

### 3.3.8 Monitoring

We keep an eye on our systems and networks to catch any problems. We use tools to watch for things like viruses and unusual activities.

#### 3.3.9 Legal Regulatory Obligations

We take our legal duties seriously. We follow rules like ISO 27001 to keep our information systems secure.

#### 3.3.10 Training and Awareness

We teach our team about staying safe with information. Everyone gets training when they start, and we update it regularly to cover new things.

### 3.4 Policy Compliance

#### 3.4.1 Compliance Measurement: Checking if We Follow the Rules

Our security team checks if we're following these rules. They might walk around, watch videos, use tools, or do audits to make sure.

#### 3.4.2 Exceptions: When We Can Bend the Rules

If we need to do something different, we ask the security team first. We can't break the rules without asking.

#### 3.4.3 Non-Compliance

If someone doesn't follow these rules, they might get in trouble. It could lead to things like talking to their manager or even losing their job.

## 4 Risk Assessment

This section focuses on understanding and managing risks at CyberGuard Innovations Ltd. It consists of two parts: qualitative risk determination and a risk register.

### 4.1 Qualitative Risk Determination

The level of risk can be determined using the following equation:

$$Risk = Impact \times Likelihood$$

Where:

- $Impact = Asset \times Threat$
- $Likelihood = Threat \times Vulnerability \times Controls$

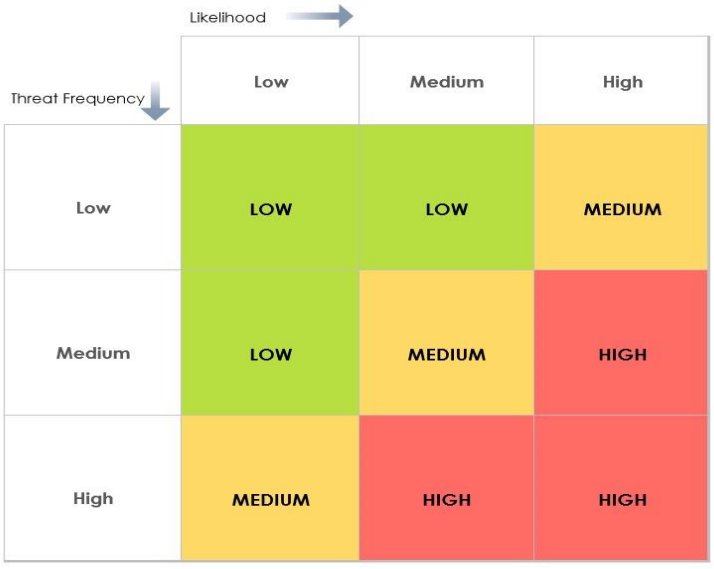
We will use qualitative ratings for the elements in the equation to determine the overall risk. The matrices presenting these qualitative ratings are shown below:

1) Resistance Strength Matrix.

**Resistance Strength**


2) Vulnerability Matrix.

**Vulnerability**




3) Exposure Matrix.

Exposure

| Asset \ Impact | Low | Medium | High |
|---|---|---|---|
| Low | LOW | LOW | MEDIUM |
| Medium | LOW | MEDIUM | HIGH |
| High | MEDIUM | HIGH | HIGH |

4) Likelihood Matrix.

Likelihood of Event

| Impact \ Risk | Low | Medium | High |
|---|---|---|---|
| Low | LOW | LOW | MEDIUM |
| Medium | LOW | MEDIUM | HIGH |
| High | MEDIUM | HIGH | HIGH |

## 4.2 RISK REGISTER

The table below shows the risk register for all assets in the hospital. It should be mentioned that:

- The **likelihood** metrics are (from lowest to highest): rare – unlikely – possible – likely – almost certain.
- The **impact** metrics are (from lowest to highest): very low – low – medium – high – very high.
- The **risk** metrics are (from lowest to highest): low – medium – high.

| # | Assets | Threat/ Vulnerabilities | Existing Controls | Likelihood | Impact | Risk | Priority (1-5) |
|---|---|---|---|---|---|---|---|
| **Hardware Assets** | | | | | | | |
| **1** | High-Performance Computing Infrastructure | Overheating, Power Outages, Hardware Failures | HVAC Systems, Power Backup | Low | High | Medium | 3 |
| **2** | Network Devices (Routers, Switches) | Unauthorized Access, Firmware Vulnerabilities, DDoS Attacks | Access Control Lists, Regular Firmware Updates | Medium | Medium | Medium | 3 |
| **3** | Servers (Local and Cloud-based) | Software Exploits, Unauthorized Access, Data Breaches | Firewalls, Intrusion Detection System (IDS) | High | High | High | 4 |
| **4** | Workstations and Laptops | Malware Infections, Phishing Attacks, Physical Theft | Antivirus Software, Email Filtering | Medium | High | Medium | 3 |
| **5** | Mobile Devices (Smartphones, Tablets) | Data Leakage, Malicious Apps, Device Loss or Theft | Mobile Device Management (MDM) Solutions | Low | High | Medium | 2 |
| **6** | Data Storage Devices (Hard Drives, SSDs) | Hacking, confidentiality, integrity, and availability concerns | Encryption, Access Controls | Low | High | Medium | 2 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **7** | Physical Security Systems (CCTV, Access Control) | Tampering, Unauthorized Access, Communication Interception | Regular Security Audits, Access Logs | Low | Medium | Low | 2 |

| **Software Assets** | | | | | | | |
|---|---|---|---|---|---|---|---|
| **8** | Operating Systems | Unpatched Vulnerabilities, Malware Exploits, Insider Threats | Regular Patch Management, Antivirus Software | Medium | High | Medium | 3 |
| **9** | Security Software (Firewalls, Antivirus) | Inadequate Configuration, Signature Lag, False Positives | Regular Configuration Audits, Real-time Updates | Low | Medium | Low | 2 |
| **10** | Database Management Systems (DBMS) | SQL Injection, Insecure Configurations, Unauthorized Access | Authentication Controls, Regular Audits | High | High | High | 5 |
| **11** | Web Applications | Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), Session Hijacking | Web Application Firewall, Code Reviews | High | High | High | 4 |
| **12** | Encryption Software | Weak Encryption Algorithms, Key Management Issues, Implementation Flaws | Strong Key Management, Regular Encryption Audits | Medium | High | Medium | 3 |
| **13** | Authentication Systems | Weak Password Policies, Credential Stuffing, Brute Force Attacks | Multi-Factor Authentication, Password Policies | High | High | High | 5 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **14** | Network Monitoring Tools | Misconfigurations, Lack of Real-time Alerts, Data Overload | Regular Configuration Checks, Real-time Alerts | Medium | Medium | Medium | 3 |
| **15** | Collaboration Software (Messaging, Video Conferencing) | Data Leakage, Unauthorized Access, Endpoint Vulnerabilities | Secure Communication Protocols, Access Controls | High | High | High | 4 |
| **16** | Backup and Recovery Software | Insufficient Backup Frequency, Lack of Encryption, Data Integrity Concerns | Regular Backup Testing, Encryption Practices | Low | High | Medium | 2 |
| **17** | Patch Management Tools | Delayed Patch Deployments, Incomplete Vulnerability Assessment, Compatibility Issues | Automated Patch Deployment, Regular Assessments | Medium | Medium | Medium | 3 |
| **Information Assets** | | | | | | | |
| **18** | Proprietary Threat Intelligence Databases | Unauthorized Access, Data Corruption, Insider Threats | Access Controls, Regular Audits | Medium | High | Medium | 3 |
| **19** | Client Confidentiality (Sensitive Cybersecurity Strategies) | Data Breaches, Insider Threats, Unauthorized Access | Encryption, Access Controls, User Authentication | Medium | High | Medium | 3 |
| **20** | Research and Development Prototypes | Intellectual Property Theft, Unauthorized Access | Secure Development Practices, Access Controls | Low | High | Low | 2 |
| **Business Assets** | | | | | | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **21** | Customer Base | Loss of Customers, Negative Feedback, Data Breaches | Customer Relationship Management, Data Encryption | Medium | High | Medium | 3 |
| **22** | Staff and Employee Information | Unauthorized Access, Data Breaches, Insider Threats | Employee Training, Access Controls | High | High | High | 4 |
| **23** | Brand Reputation | Negative Publicity, Social Media Attacks, Customer Complaints | Social Media Monitoring, Reputation Management | Low | High | Medium | 2 |

# 5 IMPLEMENTATION PLAN

The implementation plan is shown in the Statement of Applicability (SoA) for CyberGuard below. Also, will be attached.

CyberGuards: Statement of Applicability | ISO27001:2022 Annex A/ ISO27001:2022 Controls

Classification: Confidential

| ISO27002 Clause | Title | Current controls | Control Applicable ( Y/N) | Remarks (with justification for exclusions) | Remarks (overview of implementation) |
|---|---|---|---|---|---|
| 5 | organizational controls | | "Yes" | | |
| 5.1 | Policies for information security | Information security policy and topic-specific policies shall 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. | "Yes" | | Policies defined and regularly reviewed. |
| 5.2 | Information security roles and responsibilities | Information security roles and responsibilities shall be defined and allocated according to the organization needs. | Yes | | Roles and responsibilities are clearly defined and aligned with organizational needs. |
| 5.3 | Segregation of duties | Conflicting duties and conflicting areas of responsibility shall be segregated. | Yes | | Segregation of duties implemented to prevent conflicts. |
| 5.4 | Management responsibilities | Management shall require all personnel to apply information security in accordance with the established information security policy, topic-specific policies and procedures of the organization. | Yes | | Management enforces adherence to information security policies. |
| 5.5 | Contact with authorities | The organization shall establish and maintain contact with relevant authorities. | Yes | | Established and maintained contact with relevant authorities for information security matters. |
| 5.6 | Contact with special interest groups | The organization shall establish and maintain contact with special interest groups or other specialist security forums and professional associations. | Yes | | Regular contact maintained with special interest groups for security updates. |
| 5.7 | Threat intelligence | Information relating to information security threats shall be collected and analyzed to produce threat intelligence. | Yes | | Regular collection and analysis of threat intelligence for proactive security measures. |
| 5.8 | Information security in project management | Information security shall be integrated into project management. | Yes | | Information security considerations integrated into project management processes. |
| 5.9 | Inventory of information and other associated assets | An inventory of information and other associated assets, including owners, shall be developed and maintained. | Yes | | Comprehensive inventory developed and regularly updated. |
| 5.10 | Acceptable use of information and other associated assets | Rules for the acceptable use and procedures for handling information and other associated assets shall be identified, documented and implemented. | Yes | | Clear rules for acceptable use documented and implemented. |
| 5.11 | Return of assets | Personnel and other interested parties as appropriate shall return all the organization's assets in their possession upon change or termination of their employment, contract or agreement. | Yes | | Policies in place for the return of assets upon employment changes. |
| 5.12 | Classification of information | Information shall be classified according to the information security needs of the organization based on confidentiality, integrity, availability and relevant interested party requirements. | Yes | | Information classified based on confidentiality, integrity, availability, and relevant requirements. |
| 5.13 | Labelling of information | An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by the organization. | Yes | | Procedures for information labeling developed and implemented. |
| 5.14 | Information transfer | Information transfer rules, procedures, or agreements shall be in place for all types of transfer facilities within the organization and between the organization and other parties. | NO | No specific rules or agreements for information transfer established. | |
| 5.15 | Access control | Rules to control physical and logical access to information and other associated assets shall be established and implemented based on business and information security requirements. | Yes | | Rules for physical and logical access control implemented based on business and security requirements. |
| 5.16 | Identity management | The full life cycle of identities shall be managed. | NO | No full life cycle management of identities in place. | |
| 5.17 | Authentication information | Allocation and management of authentication information shall be controlled by a management process, including advising personnel on appropriate handling of authentication information. | Yes | | Allocation and management of authentication information controlled by a defined process. |
| 5.18 | Access rights | 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. | NO | Access rights not consistently provisioned, reviewed, modified, or removed based on policies. | |
| 5.19 | Information security in supplier relationships | Processes and procedures shall be defined and implemented to manage the information security risks associated with the use of supplier's products or services. | Yes | | Processes and procedures for managing security risks in supplier relationships defined and implemented. |
| 5.20 | Addressing information security within supplier agreements | Relevant information security requirements shall be established and agreed with each supplier based on the type of supplier relationship. | NO | No relevant security requirements established and agreed upon with each supplier based on the type of supplier relationship. | |
| 5.21 | Managing information security in the information and communication technology (ICT) supply chain | Processes and procedures shall be defined and implemented to manage the information security risks associated with the ICT products and services supply chain. | Yes | | Processes and procedures for managing information security risks associated with the ICT supply chain are established and implemented. |
| 5.22 | Monitoring, review and change management of supplier services | The organization shall regularly monitor, review, evaluate and manage change in supplier information security practices and service delivery. | No | Regular monitoring, review, and evaluation of supplier information security practices and service delivery are not conducted. | |
| 5.23 | Information security for use of cloud services | Processes for acquisition, use, management and exit from cloud services shall be established in accordance with the organization's information security requirements. | Yes | | Processes for acquisition, use, management, and exit from cloud services are established and followed according to information security require |
| 5.24 | Information security incident management planning and preparation | The organization shall plan and prepare for managing information security incidents by defining, establishing and communicating information security incident management processes, roles and responsibilities. | Yes | | Information security incident management processes, roles, and responsibilities are defined, established, and communicated. |
| 5.25 | Assessment and decision on information security events | The organization shall assess information security events and decide if they are to be categorized as information security incidents. | Yes | | Information security events are assessed to determine whether they should be categorized as information security incidents. |
| 5.26 | Response to information security incidents | Information security incidents shall be responded to in accordance with the documented procedures. | No | No formal mechanism for collecting and analyzing threat intelligence is established. | |
| 5.27 | Learning from information security incidents | Knowledge gained from information security incidents shall be used to strengthen and improve the information security controls. | Yes | | Knowledge gained from information security incidents is used to strengthen and improve information security controls. |
| 5.28 | Collection of evidence | The organization shall establish and implement procedures for the identification, collection, acquisition and preservation of evidence related | No | No specific plan in place for maintaining information security during disruptions. | |
| 5.29 | Information security during disruption | The organization shall plan how to maintain information security at an appropriate level during disruption. | No | | No protection measures are implemented to safeguard records from loss, destruction, falsification, unauthorized access, and unauthorized rele |
| 5.30 | ICT readiness for business continuity | ICT readiness shall be planned, implemented, maintained and tested based on business continuity objectives and ICT continuity requirements | Yes | | ICT readiness is planned, implemented, maintained, and tested based on business continuity objectives and ICT continuity requirements. |
| 5.31 | Legal, statutory, regulatory and contractual requirements | Legal, statutory, regulatory and contractual requirements relevant to information security and the organization's approach to meet these requirements shall be identified, documented and kept up to date. | No | Legal, statutory, regulatory, and contractual requirements relevant to information security are not identified, documented, and kept up-to-date. | |
| 5.32 | Intellectual property rights | The organization shall implement appropriate procedures to protect intellectual property rights. | Yes | | Intellectual property rights are protected through appropriate procedures and measures. |
| 5.33 | Protection of record | Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release | No | | No specific measures are implemented to protect records from various threats. |
| 5.34 | Privacy and protection of personal identifiable information (PII) | The organization shall identify and meet the requirements regarding the preservation of privacy and protection of PII according to applicable laws and regulations and contractual requirements. | Yes | | Privacy and protection of personally identifiable information (PII) are identified and preserved according to applicable laws, regulations, and co |
| 5.35 | Independent review of information security | The organization's approach to managing information security and its implementation including people, processes and technologies shall be reviewed independently at planned intervals, or when significant | Yes | | The organization's approach to managing information security is regularly reviewed for compliance with policies, rules, and standards. |
| 5.36 | Compliance with policies, rules and standards for information security | Compliance with the organization's information security policy, topic-specific policies, rules and standards shall be regularly reviewed. | Yes | | Operating procedures for information processing facilities are documented and available to personnel who need them. |
| 5.37 | Documented operating procedures | Operating procedures for information processing facilities shall be documented and made available to personnel who need them. | No | | No independent review of the organization's approach to managing information security is conducted. |
| 6 | People controls | | Yes | | |
| 6.1 | Screening | Background verification checks on all candidates to become personnel shall be carried out prior to joining the organization and on an ongoing basis taking into consideration applicable laws, regulations and ethics | Yes | | Background verification checks on all candidates to become personnel are carried out prior to joining the organization and ongoing basis. |
| 6.2 | Terms and conditions of employment | The employment contractual agreements shall state the personnel's and the organization's responsibilities for information security. | Yes | | The employment contractual agreements state the personnel's and the organization's responsibilities for information security. |

| ISO27002 Clause | Title | Current controls | Control Applicable ( Y/N) | Remarks (with justification for exclusions) | Remarks (overview of implementation) |
|---|---|---|---|---|---|
| 6.3 | Information security awareness, education and training | Personnel of the organization and relevant interested parties shall receive appropriate information security awareness, education and training and regular updates of the organization's information security policy, | Yes | | Personnel and relevant interested parties receive appropriate information security awareness, education, and training as relevant for their job |
| 6.4 | Disciplinary process | A disciplinary process shall be formalized and communicated to take actions against personnel and other relevant interested parties who have committed an information security policy violation | Yes | | A formal disciplinary process is formalized and communicated to take actions against personnel and other relevant interested parties for infor |
| 6.5 | Responsibilities after termination or change of employment | Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, enforced and communicated to relevant personnel and other interested parties | NO | Responsibilities and duties that remain valid after termination or change of employment are not defined, enforced, and communicated to relevant personnel and other interested parties. | |
| 6.6 | Confidentiality or non-disclosure agreements | Confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified, documented, regularly reviewed and signed by personnel and other | Yes | | Confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information are identified, documented, |
| 6.7 | Remote working | Security measures shall be implemented when personnel are working remotely to protect information accessed, processed or stored outside the organization's premises | Yes | | Security measures are implemented when personnel are working remotely to protect information accessed, processed, or stored outside the o |
| 6.8 | Information security event reporting | The organization shall provide a mechanism for personnel to report observed or suspected information security events through appropriate channels in a timely manner | Yes | | The organization provides a mechanism for personnel to report observed or suspected information security events through appropriate chann |
| 7 | Physical controls | | Yes | | |
| 7.1 | Physical security perimeters | Security perimeters shall be defined and used to protect areas that contain information and other associated as | Yes | | Security perimeters are defined and used to protect areas that contain information and other associated assets. |
| 7.2 | Physical entry | Secure areas shall be protected by appropriate entry controls and access points. | Yes | | Secure areas are protected by appropriate entry controls and access points. |
| 7.3 | Securing offices, rooms and facilities | Physical security for offices, rooms and facilities shall be designed and implem | Yes | | Physical security for offices, rooms, and facilities is designed and implemented. |
| 7.4 | Physical security monitoring | Premises shall be continuously monitored for unauthorized physic al access. | Yes | | Premises are continuously monitored for unauthorized physical access. |
| 7.5 | Protecting against physical and environmental threats | Protection against physical and environmental threats, such as natural disasters and other intentional or unintentional physical threats to infrastructure shall be designed and implemented. | NO | Protection against physical and environmental threats is not designed and implemented. | |
| 7.6 | Working in secure areas | Security measures for working in secure areas shall be designed and implemented | Yes | | Security measures for working in secure areas are designed and implemented. |
| 7.7 | Clear desk and clear screen | Clear desk rules for papers and removable storage media and clear screen rules for information processing facilities shall be defined and appropriately enforced. | Yes | | Clear desk rules for papers and removable storage media and clear screen rules for information processing facilities are defined. |

| ISO27002 Clause | Title | Current controls | Control Applicable ( Y/N) | Remarks (with justification for exclusions) | Remarks (overview of implementation) |
|---|---|---|---|---|---|
| 7.8 | Equipment siting and protection | Equipment shall be sited securely and protected | Yes | | Equipment is sited securely and protected. |
| 7.9 | Security of assets off-premises | Off-site assets shall be protected. | Yes | | Off-site assets are protected. |
| 7.10 | Storage media | Storage media shall be managed through their life cycle of acquisition, use, transportation and disposal in accordance with the organization's classification scheme and handling requirements. | Yes | | Storage media is managed through their life cycle of acquisition, use, transportation, and disposal. |
| 7.11 | Supporting utilities | Information processing facilities shall be protected from power failures and other disruptions caused by failures in supporting utilities. | Yes | | Information processing facilities are protected from power failures and other disruptions caused by failures in supporting utilities. |
| 7.12 | Cabling security | Cables carrying power, data or supporting information services shall be protected from interception, interference or damage. | Yes | | Cables carrying power, data, or supporting information services are protected from interception, interference, or damage. |
| 7.13 | Equipment maintenance | Equipment shall be maintained correctly to ensure availability, integrity and confidentiality of information. | Yes | | Equipment is maintained correctly to ensure availability, integrity, and confidentiality of information. |
| 7.14 | Secure disposal or re-use of equipment | 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. | NO | Items of equipment containing storage media are not verified to ensure that any sensitive data and licensed software have been removed or securely overwritten prior to disposal or re-use. | |
| 8 | Technological controls | | Yes | | |
| 8.1 | User end point devices | Information stored on, processed by or accessible via user end point devices shall be protected | Yes | | Information stored on, processed by, or accessible via user end point devices is protected. |
| 8.2 | Privileged access rights | The allocation and use of privileged access rights shall be restricted and managed | Yes | | The allocation and use of privileged access rights are restricted and managed. |
| 8.3 | Information access restriction | Access to information and other associated assets shall be restricted in accordance with the established topic-specific policy on access control. | Yes | | Access to information and other associated assets is restricted in accordance with the established topic-specific policy on access control. |
| 8.4 | Access to source code | Read and write access to source code, development tools and software libraries shall be appropriately managed | NO | Read and write access to source code, development tools, and software libraries are not appropriately managed. | |
| 8.5 | Secure authentication | Secure authentication technologies and procedures shall be implemented based on information access restrictions and the topic-specific policy on access control | Yes | | Secure authentication technologies and procedures are implemented based on information access restrictions and the topic-specific policy on ac |
| 8.6 | Capacity management | The use of resources shall be monitored and adjusted in line with current and expected capacity requirem | NO | The use of resources is not monitored and adjusted in line with current and expected capacity requirements. | |

| ISO27002 Clause | Title | Current controls | Control Applicable ( Y/N) | Remarks (with justification for exclusions) | Remarks (overview of implementation) |
|---|---|---|---|---|---|
| 8.7 | Protection against malwar | Protection against malware shall be implemented and supported by appropriate user awareness. | Yes | | Protection against malware is implemented and supported by appropriate user awareness. |
| 8.8 | Management of technical vulnerabilities | Information about technical vulnerabilities of information systems in use shall be obtained, the organization's exposure to such vulnerabilities shall be evaluated and appropriate measures shall be take | Yes | | Information about technical vulnerabilities of information systems in use is obtained, and appropriate measures are taken. |
| 8.9 | Configuration management | Configurations, including security configurations, of hardware, software, services and networks shall be established, documented, implemented, monitored and reviewed. | Yes | | Configurations, including security configurations, of hardware, software, services, and networks are established, documented, implemented, r |
| 8.1 | Information deletion | Information stored in information systems, devices or in any other storage media shall be deleted when no longer required. | Yes | | Information stored in information systems, devices, or in any other storage media is deleted when no longer required. |
| 8.110 | Data masking | 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 | Yes | | Data masking is used in accordance with the organization's topic-specific policy on access control and other related topic-specific policies, and b |
| 8.12 | Data leakage prevention | Data leakage prevention measures shall be applied to systems, networks and any other devices that process, store or transmit sensitive information | NO | Data leakage prevention measures are not applied to systems, networks, and any other devices that process, store, or transmit sensitive information. | |
| 8.13 | Information backup | Backup copies of information, software and systems shall be maintained and regularly tested in accordance with the agreed topic-specific policy on backup. | Yes | | Backup copies of information, software, and systems are maintained and regularly tested in accordance with the agreed topic-specific policy on |
| 8.14 | Redundancy of information processing facilities | Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements | Yes | | Information processing facilities are implemented with redundancy sufficient to meet availability requirements. |
| 8.15 | Logging | Logs that record activities, exceptions, faults and other relevant events shall be produced, stored, protected and analysed | Yes | | Logs that record activities, exceptions, faults, and other relevant events are produced, stored, protected, and analyzed. |
| 8.16 | Monitoring activities | Networks, systems and applications shall be monitored for anomalous behaviour and appropriate actions taken to evaluate potential information security incidents. | Yes | | Networks, systems, and applications are monitored for anomalous behavior, and appropriate actions are taken to evaluate potential informatio |
| 8.17 | Clock synchronization | The clocks of information processing systems used by the organization shall be synchronized to approved time sources | Yes | | The clocks of information processing systems used by the organization are synchronized to approved time sources. |
| 8.18 | Use of privileged utility programs | The use of utility programs that can be capable of overriding sy | NO | The use of utility programs capable of overriding system and application controls is not appropriately restricted. | |
| 8.19 | Installation of software on operational systems | Procedures and measures shall be implemented to securely manage software installation on operational syst | NO | Procedures and measures to securely manage software installation on operational systems are not effectively implemented. | |
| 8.20 | Networks security | Networks and network devices shall be secured, managed and controlled to protect information in systems and applications | Yes | | Networks and network devices are secured, managed, and controlled to protect information in systems and applications. |

| ISO27002 Clause | Title | Current controls | Control Applicable ( Y/N) | Remarks (with justification for exclusions) | Remarks (overview of implementation) |
|---|---|---|---|---|---|
| 8.21 | Security of network services | Security mechanisms, service levels and service requirements of network services shall be identified, implemented and monitored | NO | Security mechanisms, service levels, and service requirements of network services are not identified, implemented, and monitored effectively. | |
| 8.22 | Segregation of networks | Groups of information services, users and information systems shall be segregated in the organization's networks. | Yes | | Groups of information services, users, and information systems are segregated in the organization's networks. |
| 8.23 | Web filtering | Access to external websites shall be managed to reduce exposure to malicious content. | NO | Access to external websites is not effectively managed to reduce exposure to malicious content. | |
| 8.24 | Use of cryptography | Rules for the effective use of cryptography, including cryptographic key management, shall be defined and implemented | Yes | | Rules for the effective use of cryptography, including cryptographic key management, are defined and implemented. |
| 8.25 | Secure development life cycle | Rules for the secure development of software and systems shall be established and applied | Yes | | Rules for the secure development of software and systems are established and applied. |
| 8.26 | Application security requirements | Information security requirements shall be identified, specified and approved when developing or acquiring applications | Yes | | Information security requirements are identified, specified, and approved when developing or acquiring applications. |
| 8.27 | Secure system architecture and engineering principles | Principles for engineering secure systems shall be established, documented, maintained and applied to any information system development activities | NO | Principles for engineering secure systems are not effectively established, documented, maintained, and applied to any information system development activities. | |
| 8.28 | Secure coding | Secure coding principles shall be applied to software development | Yes | | Secure coding principles are applied to software development. |
| 8.29 | Security testing in development and acceptance | Security testing processes shall be defined and implemented in the development life cycle. | NO | Security testing processes are not effectively defined and implemented in the development life cycle. | |
| 8.30 | Outsourced development | The organization shall direct, monitor and review the activities related to outsourced system development. | Yes | | The organization directs, monitors, and reviews activities related to outsourced system development. |
| 8.31 | Separation of development, test and production environments | Development, testing and production environments shall be separated and se | NO | Development, testing, and production environments are not effectively separated and secured. | |
| 8.32 | Change manageme | Changes to information processing facilities and information systems shall be subject to change management procedures. | Yes | | Changes to information processing facilities and information systems are subject to change management procedures. |
| 8.33 | Test information | Test information shall be appropriately selected, protected and managed | Yes | | Test information is appropriately selected, protected, and managed. |
| 8.34 | Protection of information systems during audit testing | Audit tests and other assurance activities involving assessment of operational systems shall be planned and agreed between the tester and | NO | Audit tests and other assurance activities involving assessment of operational systems are not effectively planned and agreed between the tester and appropriate management. | |