Presidency of the Cabinet of Ministers
The Egyptian Supreme Cybersecurity Council

The Essential Cybersecurity Controls

(1st version)

TLP: Green

The traffic light Protocol (tlp)

The Traffic Light Protocol (TLP) was created in order to facilitate greater sharing of information. TLP is a set of designations used to ensure that sensitive information is shared with the appropriate audience. It employs four colors to indicate expected sharing boundaries to be applied by the recipient(s). The protocol includes four colors (traffic lights), which are detailed as follows:

Red- Not for disclosure, restricted to participants only:
Sources may use TLP:RED when information cannot be effectively acted upon by additional parties. Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed

Amber- Limited disclosure, restricted to participants' organizations:

Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved. Recipients may only share TLP: AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm.

Green- Limited disclosure, restricted to the community:

Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector. Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels.

White- Disclosure is not limited:
Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. TLP:WHITE information may be distributed without restriction.

TABLE OF CONTENTS

Executive Summary

The objectives of the Egyptian Supreme Cybersecurity Council (ESCC) are consistent and harmonious with the State's adoption of Digital Transformation, the establishment of 'Digital Egypt', and 'Secure Digital Egypt' Vision, and the exertion of best efforts to keep pace with all technological developments in information technology services. Consequently, it was required to secure the communications and information infrastructure so that a safe digital ecosystem could be built and fostered for various sectors to be able to provide integrated e-services.

In view of the Council's vision of the paramount importance of cybersecurity, it has developed cybersecurity frameworks, standards, controls and policies that must be implemented in all organizations and institutions throughout the country.

Within the framework of its keenness to promote cybersecurity and secure its networks, systems and electronic data, the Council has developed the Essential Cybersecurity Controls (2023), which stipulate the minimum cybersecurity requirements, that should be observed in the State's organizations and institutions that fall within the scope of these controls. This document provides all the provisions, scope of work and objectives of these Controls, in addition to compliance and follow-up mechanisms.

All State's organizations and institutions must comply with these Controls and take on their responsibilities towards hardening Egypt's cyberspace by boosting their cybersecurity level and securing their systems, networks and electronic data, and observing the standards, frameworks, policies and controls issued by the Council in this respect.

Introduction

The Egyptian Supreme Cybersecurity Council (ESCC), pursuant to the Cabinet of Ministers' Decree No. 2259 of 2014, is the official authority competent to develop the national cybersecurity strategy to combat cyber threats and attacks, supervise its implementation and updating, approve the identification of critical communications and information infrastructure in all State's sectors, develop frameworks for assessing and following up on their security and protection. In addition, the ESCC is mandated to approve frameworks, strategies and policies for securing the critical communications and information infrastructure, develop plans and programs to enhance cybersecurity industry, and the standards binding on all parties, setting them as the minimum requirements for securing the critical infrastructure for communications and information, and compelling them to take the measures needed to ensure the highest level of safety and protection for Egypt's cyberspace. In compliance with the State's adoption of Digital Transformation and the pressing need for ensuring cybersecurity governance, and securing and protecting information assets, mitigating cyber risks, and promoting cyber

resilience and business continuity, the Council has developed the Essential Cybersecurity Controls Proposal, as per the best practices and the approach embraced by other countries to develop these controls and in compliance with the international standards ISO/IEC 27001:2022, ISO/IEC 27002:2022 and the Special Publication (SP) 800-53 (Revision 5) published by the National Institute of Standards and Technology (NIST).

The Objectives

Developing the minimum essential cybersecurity requirements for cybersecurity protection and enhancement in the State's organizations and institutions to secure their networks and systems. In addition, there are three main cybersecurity pivots that should be taken into consideration to secure information and technical assets:

- Persons;
- Procedures and processes;
- Technological Measures.

These Controls as well aim to:

- Mitigate cyber risks and maintain the government's ability to carry out its tasks.
- Propagate awareness about cyber security in society.
- Improve cyber resilience and business continuity despite cyber threats.

Scope

These Controls are applicable to the government institutions in the Arab Republic of Egypt, their representatives, and those acting on their behalf, affiliated entities and other institutions who have been granted access to information technology and communications systems therein. It is recommended to be guided by these Controls in implementing best cybersecurity practices.

Classification of Cyber Security Controls

These Controls are classified into the following five (5) Main Domains as per cyber security concepts:

1) Identify:
Developing Regulatory Insight Into Managing Cybersecurity Risks that Threaten Systems, Assets and Resources.

2) Protect:
Developing the Entities' Capabilities and Developing the Necessary Security Measures to Protect and Secure Systems and Assets

3) Detect
Developing and Implementing the Appropriate Activities Required to Detect Suspected Events and Cyber Threats.

4) Respond:
Taking the Required Measures to Encounter Cyber Incidents and Threats.

5) Recovery:
Developing and Implementing the Appropriate Activities Required to Maintain Resilience Plans and Recover any Capabilities or Services that have been Hampered due to Cybersecurity Incidents.

1

(Identify)

Developing Regulatory Insight into Managing Cybersecurity Risks that Threaten Systems, Assets and Resources.

2

(Protect)

Developing the Entities' Capabilities and Developing the Necessary Security Measures to Protect and Secure Systems and Assets

3

(Detect)

Developing and Implementing the Appropriate Activities Required to Detect Suspected Events and Cyber Threats.

4

(Respond)

Taking the Required Measures to Encounter Cyber Incidents and Threats.

5

(Recovery)

Developing and Implementing the Appropriate Activities Required to Maintain Resilience Plans and Recover any Capabilities or Services that have been Hampered due to Cybersecurity Incidents.

Figure (1): The Main Domains

The Essential Cybersecurity Controls Proposal comprises the following:

- **Five (5) Main Domains for the essential cybersecurity controls.**
- **Sixteen (16) Sub-domains of the essential cybersecurity controls.**
- **Ninety-eight (98) controls.**

Figure (2): The Sub-Domains

Identify- Protect-Detect-Respond-Recovery

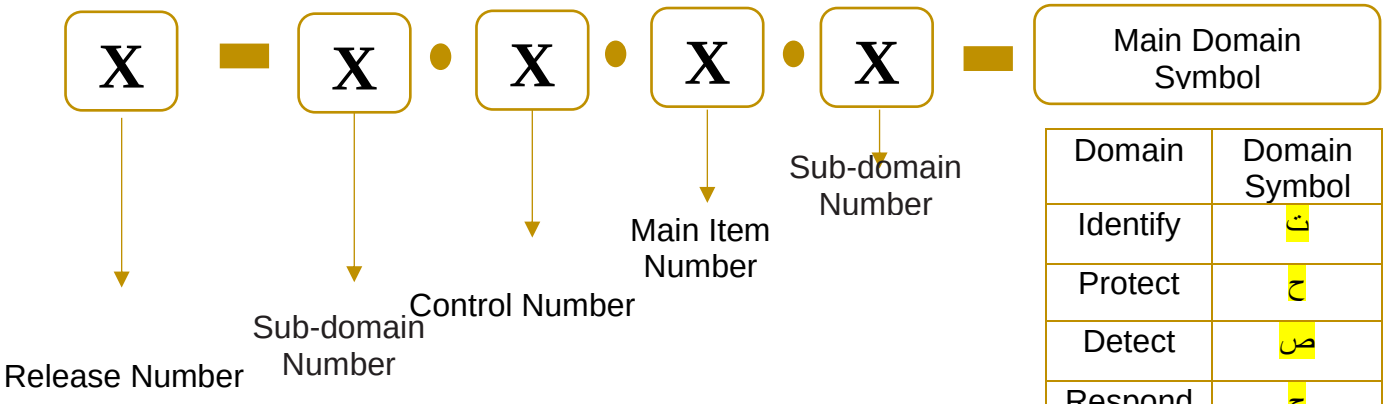
Identify: Governance- Asset Management Security in Supplier Relationships- Legal Affairs and Compliance

Protect: Identity and Access Management- Information Protection - Human Resources Security- Physical Security- Secure Configurations- Networks and Systems Security-Applications Security

Detect: Threats and vulnerabilities Management Cybersecurity Events Management

Respond: Incident Management
Recovery: Continuity- Cybersecurity Resilience

Figure (3) displays how the controls or items are referred to:



Domain	Domain Symbol
Identify	ت
Protect	ح
Detect	ص
Respond	ج
Recovery	ع

Figure (3) - Reference to Controls and Items

The following table demonstrates the controls structure:

Table (1) Controls Reference Table

Main Domain Name	Main Domain No,

Sub-Domain Name .Sub-Domain Number	
Control No./Name	Sub-Domain Number .Domain Number Domain Name
Purpose	Control purpose
Control Description	Sub-domain Number - Control Number- Control Item Number - Control Content: Control Sub-item Number – Control Sub-item Content

Identify

Developing Regulatory Insight Into Managing Cybersecurity Risks that Threaten Systems, Assets and Resources.

Identify 1

1. Governance

Control No./Name	1.1 Cybersecurity Policies
Purpose	To ensure the efficiency and continuity of the cybersecurity management and support system as per the entity's requirements or the relevant legislative or regulatory requirements.
Control Description	1.1.1. The Cybersecurity Policy and the topic-specific policies should be applicable and implemented, as a minimum, as follows: 1. identified and approved by the relevant cybersecurity department. 2. published and endorsed by the relevant employees and interested parties. 3. reviewed periodically or in case any changes are made to the entity's requirements or the relevant legislative or regulatory requirements. 4. determine the purpose, scope, roles, responsibilities, management commitment, coordination between regulatory authorities and how to comply to these policies. 5. consistent with the applicable laws, orders, executive regulations, policies, standards, and instructions. 6. The entity should develop relevant measures that enable and facilitate the implementation of the Policy and relevant controls. 7. supported with technical and security standards (e.g., standards for cryptography, operating systems, and databases).
Control No./Name	1.2 Cybersecurity Roles and Responsibilities
Purpose	To ensure that the roles and responsibilities of all relevant parties involved in the implementation, operation and management of cybersecurity controls are identified in the entity through a definite and approved organizational structure.
Control Description	1.2.1 The cybersecurity roles and responsibilities should be identified, distributed and reviewed in accordance with the entity's needs. 1.2.2 The authorization levels should be identified and documented in accordance with the skills required for the role; those authorizations should be reviewed and updated at definite intervals while enhancing and improving the skills of the relevant staff.
Control No./Name	1.3 Administrative Responsibilities

Purpose	To ensure that the entity's management is aware of its cybersecurity role and has taken the necessary measures to make sure that all employees are aware of and complying with their cybersecurity responsibilities.
Control Description	1.3.1 The management should require all personnel to abide by the cybersecurity responsibilities in accordance with the topic-specific policies and procedures applicable in the entity. 1.3.2 The management's responsibilities should include, as a minimum, the following: 1. The provision of guidelines and instructions to them on their roles and responsibilities related to cybersecurity before giving them access to the entity's information and other associated assets. 2. The compliance with the terms and conditions of employment and contract conditions, including the entity's Information Security Policy. 3. The provision of a confidential channel for reporting any violations related to cybersecurity.
Control No./Name	1.4 Contacting with Relevant Authorities and Interested Parties
Purpose	To ensure that the appropriate flow of information is maintained with regard to cybersecurity.
Control Description	1.4.1 The entity should develop an updated list of liaison points, through which communication takes place with the relevant authorities (Contact with Authorities), stakeholders or other cybersecurity entities and organizations.
Control No./Name	1.5 Cybersecurity in Project Management
Purpose	To ensure effective management of cybersecurity risks in the entity's projects.
Control Description	1.5.1 The cybersecurity requirements should be incorporated in the entity's project management. 1.5.2 The project management should determine, as a minimum, the following: • Cybersecurity risks; these risks should be assessed and reviewed at an early stage and on a regular basis. • Cybersecurity requirements; they should be addressed throughout the project's life cycle.
Control No./Name	1.6 The Independent Review of Cybersecurity
Purpose	To ensure the continuity of the ability, adequacy and effectiveness of the entity's and approach of cybersecurity management.

Control Description	1.6.1 An independent review of the entity's approach of cybersecurity management and implementation should take place at scheduled intervals or upon the occurrence of major changes. 1.6.2 The review should comprise the assessment of the possibility of improving and changing of the cybersecurity management approach, including the revision and update of general policies, topic-specific policies, in addition to the relevant and applicable cybersecurity controls. 1.6.3 It should be ensured that the independent auditor is provided with adequate information to complete the auditing process, or has been granted the authority required to obtain the information.
Control No./Name	1.7 Documentation of Operation Procedures
Purpose	To ensure correct and safe operation of information processing services.
Control Description	1.7.1 The operation procedures for information processing services should be documented and made available to the personnel who need them. 1.7.2 The documented operation procedures should be reviewed and updated as required. 1.7.3 The necessary authorizations should be obtained and documented before implementing any changes to the documented operation procedures.
Control No./Name	1.8 Capacity Management
Purpose	To ensure availability of the capacity needed for information processing and other processes.
Control Description	1.8.1 Capacity Management should be tuned and monitored as per the current and future capacity requirements to ensure the system performance, as required. 1.8.2 The entity should allocate a storage capacity for logs and records. 1.8.3 The entity should manage the capacity, bandwidth to reduce any impact of Denial of Service (DoS) attacks.
Control No./Name	1.9 Cybersecurity Management
Purpose	To ensure the support, management and implementation of cybersecurity programs in the entity in accordance with the cybersecurity requirements.
Control Description	1.9.1 An independent Cybersecurity Department should be established in the entity; it will be separate from the Information Technology Department, and reports directly to the entity's CEO. 1.9.2 All staff of the Cybersecurity Department should be full-time employees, and highly skilled in the field of cybersecurity. 1.9.3 A committee must be formed to supervise cybersecurity; it will be report to the entity's CEO. The members of the committee and their duties should be

	identified and documented, provided that the director of the cybersecurity department is one of the committee's members.
Control No./Name	1.10 Cybersecurity Risks Management
Purpose	To reduce cybersecurity risks that the entity might encounter and diminish their impacts.
Control Description	1.10.1 The method and measures for cybersecurity risks management should be implemented in the entity by the cybersecurity department. 1.10.2 A time schedule should be set for reviewing the method and procedures for cybersecurity risks management; they should be updated periodically, or in case changes are made to the relevant policies, controls and legislations. These changes should be documented and approved.

Identify 1

2. Asset Management

Control No./Name	2.1 Inventory of Information and Other Associated Assets
Purpose	To identify the entity's information and other associated assets, and their owners (Asset Owners) to fulfill the cybersecurity requirements.
Control Description	2.1.1 An inventory of information and other associated assets should be established; it should include, as a minimum, the following: 1. Digital assets and other related assets. 2. The classification of assets as per confidentiality, integrity and availability. 3. The type and description of assets. 4. The owner of assets, who is responsible for them. 5. The location of assets and its type. 6. The date of the inventory. 2.1.2 The inventory of the information and other associated assets should be accurate, up-to-date, and consistent with other inventories. 2.1.3 The defined information and other associated assets should be reviewed regularly in accordance with the inventory list. 2.1.4 The asset's owner shall be responsible for the appropriate management and protection of the asset.
Control No./Name	2.2 The Acceptable Use of Information and Other Associated Assets
Purpose	To ensure acceptable protection, use and handling of the information and other associated assets.
Control Description	2.2.1 The rules for the acceptable use and procedures for handling information and other associated assets should be identified, documented, and implemented. 2.2.2 The entity should develop the applicable topic-specific policy on the acceptable use of information and other associated assets; it should be announced and communicated to any personnel using or dealing with the information and other associated assets.
Control No./Name	2.3 Return of Assets

Purpose	To ensure the protection of the entity's assets as part of the change or termination of employment, contract or agreement.
Control Description	2.3.1 Employees and other interested parties should return all the entity's assets in their possession, in the event of change or termination of their employment or contract. 2.3.2 In case there is change or termination of the employees' employment, the following measures must be taken, as a minimum: 1. Disabling the employee's access to the system within a period of time to be determined by the entity. 2. Terminating or invalidating any accounts or credentials of the employee that enable him to access systems. 3. Retrieving all digital systems of the employee; including cybersecurity systems. 4. Enabling the entity to access the information and systems of any employee whose employment is terminated. 2.3.3 The entity should prevent the unauthorized copying of information (e.g., intellectual property) by terminated employees pursuant to a termination notice either during the notice period or thenceforth.
Control No./Name	2.4 Redundancy of Information Processing Facilities
Purpose	To ensure the continuous operation of information processing services.
Control Description	2.4.1 Redundancy of information Processing Facilities should be developed when initiating information processing services in order to satisfy the availability requirements. 2.4.2 The entity should establish and implement the procedures needed to activate the processing systems and the redundant components and information facilities when required. 2.4.3 Mechanisms should be established to alert the entity to any disruption of information processing services in order to enable the implementation of the planned procedures and to allow the continued availability during the repair or replacement of information processing services, when required. 2.4.4 Redundant information systems should be tested, preferably in production mode, to ensure the failover works as intended.

Identify 1

3. Security in Supplier Relationships

Control No./Name	3.1 Maintaining Cybersecurity in Supplier Relationships
Purpose	To ensure the implementation of cybersecurity requirements with regard to supplier relationships.
Control Description	3.1.1 The processes and procedures should be identified, documented, and implemented in order to manage cybersecurity risks related to the use of the supplier's products or services, including cloud computing services. They should be periodically reviewed. 3.1.2 The entity should establish a topic-specific policy on implementing and meeting the cybersecurity requirements concerning the supplier relationships.
Control No./Name	3.2 Incorporating Cybersecurity Requirements in Supplier Contracts
Purpose	To ensure the implementation of cybersecurity requirements in supplier relationships.
Control Description	3.2.1 The relevant cybersecurity requirements should be established and agreed upon with each supplier as per the type of service that the supplier provides. 3.2.2 The supplier agreements should include articles that ensure that there is a clear understanding between the entity and the supplier concerning the obligations of both parties to satisfy and document the cybersecurity requirements. 3.2.3 The terms and articles of technical specifications, contracts and agreements with suppliers should include, as a minimum, the following: 1. A description and classification of the information that will be made available or accessed. 2. The mechanism of access to information and its availability. 3. The requirements and procedures for cybersecurity incident management. 4. The right to audit the supplier's processes and cybersecurity-relevant controls; 5. The information transfer controls to secure information during physical or logical transmission.

	6. The termination clauses upon concluding agreement; including records and logs management, return of assets, safe disposal of information and other associated assets in addition to the confidentiality obligation. 7. The submission of a report on technical vulnerabilities immediately upon their detection, and how to encounter and address them. 3.2.4 The entity should establish and keep a log of agreements with external parties (such as contracts, memorandums of understanding (MoUs) and information exchange agreements) in order to keep track of its information. 3.2.5 The entity should review, check, verify and update its agreements with external parties regularly to ensure their conformity with cybersecurity requirements. 3.2.6 It must be ensured that the controls incorporated in the direct supplier contracts are also included in the contracts concluded with subcontractors.
Control No./Name	3.3 Cybersecurity Management in ICT Supply Chain
Purpose	To ensure the fulfillment and implementation of cybersecurity requirements in supplier relationships.
Control Description	3.3.1 The processes and procedures should be identified and implemented to manage cybersecurity risks related to the supply chain of ICT products and services.
Control No./Name	3.4 Monitoring, Reviewing, Assessing and Managing Change in Supplier Services
Purpose	To ensure the implementation of cybersecurity requirements in supplier relationships.
Control Description	3.4.1 The entity should periodically monitor, review, assess and manage the change in the cybersecurity practices related to supplier services.
Control No./Name	3.5 Cybersecurity Requirements for Cloud Computing Services Usage
Purpose	To identify and manage cybersecurity for the use of cloud computing services.
Control Description	3.5.1 The cybersecurity requirements of the entity should be incorporated in the processes of acquisition, use, management, and exit of the cloud computing services. 3.5.2 The entity should develop a topic-specific policy on the use of cloud computing services for all relevant interested parties and communicate it to them. 3.5.3 The entity should identify the process of management of cybersecurity risks related to cloud computing services use and communicate it to them. 3.5.4 The cybersecurity responsibilities of both the cloud computing service provider and the entity, acting as the cloud service customer, should be identified and implemented.

	3.5.5 The agreement should include the cybersecurity requirements and obligations of the cloud computing service provider and the entity, acting as the cloud service customer. 3.5.6 The entity, as the cloud service customer, should consider whether the agreement should require the cloud computing service providers to send in advance a notification before making any (technical, geographic or contractual) changes that have impacts on the service provided to the entity.
Control No./Name	3.6 Outsourced Software Development
Purpose	Ensuring the implementation of the entity's cybersecurity requirements related to outsourced software development.
Control Description	3.6.1 The entity should manage, monitor and review the activities related to outsourced software development. 3.6.2 The outsourced software development contracts should include, as a minimum, the following: 1. The terms related to licensing, code ownership, and intellectual property rights. 2. The items related to cybersecurity requirements and all phases of secure software development and relevant audit processes. 3. The items related to software checking upon receiving it to ensure that it is free from malware and vulnerabilities. 4. The items related to the development phases documentation, the needed configurations, and cybersecurity requirements during various phases of outsourced software development. 5. The items related to quality standards for receiving outsourced software. 3.6.3 The outsourcing of the development of software, its components and relevant data should be documented, monitored and maintained.

Identify

1

4. Legal Affairs and Compliance

Control No./Name	4.1 The Legal, Legislative, Regulatory and Contractual Requirements
Purpose	To ensure compliance with the cybersecurity-relevant legal, legislative, regulatory and contractual requirements.
Control Description	4.1.1 The cybersecurity-relevant legal, legislative, regulatory and contractual requirements and the method pursued by the entity should be identified to fulfill, document and update these requirements. 4.1.2 Cryptographic controls should be used in accordance with all applicable agreements, legislation and regulations.
Control No./Name	4.2 Intellectual Property Rights
Purpose	To ensure compliance with the legal, legislative, regulatory and contractual requirements relating to intellectual property rights and the usage of proprietary products.
Control Description	4.2.1 The entity should implement and document the proper procedures to protect the intellectual property rights.
Control No./Name	4.3 Protection of Privacy and Personally Identifiable information (PII)
Purpose	To ensure compliance with the legal, legislative, regulatory and contractual requirements relating to cybersecurity aspects to protect the personally identifiable information (PII).
Control Description	4.3.1 The requirements relating to the protection of privacy and the personally identifiable information (PII) should be identified in accordance with the applicable laws, contractual requirements and regulations. 4.3.2 A policy on the personally identifiable information (PII) protection shall be developed and communicated to all relevant interested parties. 4.3.3 The procedures for the protection of privacy and the personally identifiable information (PII) protection shall be developed, implemented and communicated to all interested stakeholders. 4.3.4 The appropriate technical and regulatory procedures shall be implemented to protect the personally identifiable information (PII).
Control No./Name	4.4 Compliance with Cybersecurity Policies, Rules and Standards

Purpose	To ensure the implementation and operation of cybersecurity requirements in accordance with the entity's cybersecurity policy, topic-specific policies, and the applicable rules and standards.
Control Description	4.4.1 The compliance with the entity's cybersecurity policy, topic-specific policies and the applicable rules and standards should be periodically reviewed. 4.4.2 In case non-compliance with the entity's cybersecurity policies, special policies, rules and applicable standards is proven, as a minimum, the following should be implemented: 1. Identifying and documenting the reasons for non-compliance with cybersecurity requirements. 2. Assessing, implementing and documenting the needed corrective measures to attain compliance with the cybersecurity requirements and ensure the efficiency of such corrective measures within the time period determined by the entity. 3. Reviewing the corrective measures to verify their efficiency, and identify any vulnerabilities. 4.4.3 The procedures for compliance review and monitoring should be periodically assessed and checked.

2 Protect

Protect

Developing the Entities' Capabilities and Developing the Necessary Security Measures to Protect and Secure Systems and Assets

1. Identity and Access Management

Control No./Name	1.1 Segregation of Duties
Purpose	To ensure that the risks of fraud, error and unauthorized access are minimized.
Control Description	1.1.1 Conflicting duties and areas of responsibility should be separated (Segregation of Duties). 1.1.2 The entity should identify and document the tasks and areas of responsibility that must be separated; this includes, but not limited to: 1. The software design, development and review processes. 2. The applications development and database management. 1.1.3 Users must be allowed to access systems (System Access Authorizations) in accordance with the Segregation of Duties rules applicable in the entity. 1.1.4 Activities and auditing should be monitored, and management supervision should be provided.
Control No./Name	1.2 Access Control
Purpose	To ensure the authorized access and prevention of unauthorized access to information and other associated assets.
Control Description	1.2.1 The rules that control Physical and Logical Access (Access Control Rules) to information and other associated assets should be established and implemented as per the business and cybersecurity requirements. 1.2.2 The Access Control Policy should be established and communicated to all relevant interested parties. 1.2.3 Access to the systems should only be granted as per the “need-to-know” and “need-to use” principles. 1.2.4 The entity should adopt the Least Privilege principle, allowing only authorized access to users (or the processes acting on behalf of users) to carry out specific tasks. 1.2.5 Documented procedures and specific responsibilities should be established to control access to systems.
Control No./Name	1.3 Identity Management
Purpose	To ensure the identification of individuals and systems (Identity Management) that access the entity's information and other associated assets to provide the appropriate Assignment of Access Rights.
Control Description	1.3.1 The entity should manage the full life cycle of identities from their creation until their termination. 1.3.2 The Identity Management processes should include, as a minimum, the following:

	1. Each identity should be associated with only one user, who will become responsible and accountable for the actions to be carried out with this specific identity. 2. That shared identities will be only allowed, when necessary, within the limits of business requirements, on condition that they are determined and documented beforehand. 3. The identities should be disabled or removed by the entity if they are no longer required within a definite period of time. 4. The records of all significant events relating to the use and management of user identities and authentication information should be kept and maintained.
Control No./Name	1.4 Authentication Information
Purpose	To ensure the proper entity authentication and preventing the authentication process failures.
Control Description	1.4.1 The entity should develop administrative processes for authentication information management. 1.4.2 The entity should raise the employees' awareness of the appropriate handling and protection of authentication information. 1.4.3 The entity should develop a technical system for managing users' passwords as per the entity's cybersecurity requirements.
Control No./Name	1.5 Access Rights
Purpose	To ensure access to information and other associated assets in accordance with business requirements.
Control Description	1.5.1 Access rights to information and other associated assets should be provided, managed, reviewed, modified and removed in accordance with the entity's applicable topic-specific policies and access control rules. 1.5.2 The physical and logical access rights should be reviewed regularly. 1.5.3 User's access rights to information and other associated assets should be reviewed; they should be considered for modification or removal prior to any job change or contract termination. 1.5.4 The activities of accounts creating, modifying, enabling, disabling and removing should be reviewed and verified by the entity.
Control No./Name	1.6 Privileged Access Rights
Purpose	To ensure that only authorized users, software or services are granted Privileged Access Rights.

Control Description	1.6.1 The allocation and use of Privileged Access Rights should be restricted and managed in accordance with the Access Control Policy and applicable topic-specific policies.
Control No./Name	1.7 Restricting Access to Information
Purpose	To ensure only authorized access and preventing unauthorized access to information and other associated assets.
Control Description	1.7.1 Access to information and other associated assets should be restricted in accordance with the entity's access control policy. 1.7.2 The relevant procedures should be developed, and mechanisms should be implemented to make sure that access is restricted to every access request before its enforcement and implementation by the entity.
Control No./Name	1.8 Access to Source Code
Purpose	To prevent the initiation of unauthorized functions, avoiding unintentional or malicious modifications and maintaining confidentiality and intellectual property rights.
Control Description	1.8.1 Read and write access to source code, development tools and software libraries should be properly managed.
Control No./Name	1.9 Secure Authentication
Purpose	To ensure that a user or an entity is securely authenticated when access to systems, applications, and services is granted.
Control Description	1.9.1 Secure authentication techniques and procedures should be implemented in accordance with the applicable information access restrictions, access control policy and topic-specific policies. 1.9.2 Access to information should be controlled by implementing secure login procedures, taking into consideration, as a minimum, the following: 1. Limiting the number of repetitive invalid login attempts by the user during a specific period of time, after which the account will be locked for a certain duration, and the administrator should be notified when the maximum number of unsuccessful attempts is exceeded. 2. Not displaying system information on the authentication process in order to protect the information from potential manipulation and use by unauthorized users (e.g., in case there is an error condition, the system should not point out which part of data is correct or incorrect).

	3. Recording system login attempts, whether successful or unsuccessful. 4. Not displaying passwords in clear text when entered, as well as not sending passwords in clear text over a network to avoid capture by unauthorized individuals.

Protect 2

3. Information Protection

Control No./Name	3.1 Information Classification
Purpose	To ensure identification and understanding of information protection requirements in accordance with their significance to the entity.
Control Description	3.1.1 The information and systems should be classified and documented in accordance with the entity's cybersecurity requirements on the basis of confidentiality, integrity, availability, and the requirements of the relevant interested parties. 3.1.2 The entity should develop a topic-specific policy on information classification and communicate it to all interested parties. 3.1.3 Data and information ownership should be identified.
Control No./Name	**3.2 Labeling of Information**
Purpose	To facilitate information classification and supporting the automation of information processing and management.
Control Description	1.2.1 An appropriate set of procedures for Information Labeling should be developed and implemented in accordance with the information classification plan approved and adopted by the entity. All relevant interested parties should be communicated thereof. 1.2.2 All personnel should be provided with the necessary training to ensure the proper classification and labeling of information and that they are correctly handled accordingly.
Control No./Name	**1.3 Information Transfer**
Purpose	To maintain that the transfer of information securely within the entity and with any external interested party.

Control Description	2.3.1 The Information Transfer rules, procedures or agreements should be applied for all types of transfer facilities in the entity and between the entity and other parties.

Control No./Name	2.4 Records Protection
Purpose	To ensure compliance with the legal, legislative, regulatory and contractual requirements relating to records protection and availability.
Control Description	2.4.1 Records should be protected against loss, damage, forgery, unauthorized access, and unauthorized release. 2.4.2 The entity should set a schedule for records retention that determines the records to be retained and their retention period. 2.4.3 The entity should properly destroy records after the retention period if they are no longer needed by the entity. 2.4.4 Alert notifications should be issued to the entity's competent employees upon detecting unauthorized access, modification, or deletion of audit information of records.
Control No./Name	2.5 User Endpoint Devices
Purpose	To ensure the protection of information from the risks ensuing from the use of endpoint devices.
Control Description	2.5.1 The information stored on, processed by or accessed through the User Endpoint Devices should be protected. 2.5.2 The entity should set a policy on the control and secure handling of user endpoint de peripheral devices as per the cybersecurity requirements. It should include, as a minimum, the following: 1. Software Installation Restriction. 2. The cybersecurity requirements relating to the user endpoint device software (including the software versions) and the obligation to apply the necessary updates (such as enabling automatic updating). 3. Malware protection.
Control No./Name	2.6 Protection Against Malware
Purpose	To ensure that information and other associated assets are protected from malware.

Control Description	2.6.1 Users should be protected against malware; this should be supported by appropriately raising awareness. 2.6.2 The malware detection software should be installed and updated. 2.6.3 Computers and electronic storage media should be scanned regularly to detect and remove any malware. 2.6.4 Emails, especially phishing emails and spam emails, should be filtered by using most advanced email protection techniques and mechanisms.
Control No./Name	2.7 Information Deletion
Purpose	To prevent leakage or exposure of sensitive information and ensuring compliance with legal, legislative, regulatory and contractual requirements relating to information deletion.
Control Description	2.7.1 The information stored in information systems, devices, or any other storage media should be deleted when it is no longer needed, as per the Data Retention Policy applicable in the entity.
Control No./Name	2.8 Data Masking
Purpose	To limit the leakage and exposure of sensitive data, including personally identifiable information (PII), and ensure compliance with legal, legislative, regulatory and contractual requirements.
Control Description	2.8.1 Data masking should be carried out in accordance with the entity's access control policy, other relevant topic-specific policies and business requirements and in compliance with the applicable legislations.
Control No./Name	2.9 Prevention of Data Leakage
Purpose	To ensure the detection and prevention of data leakage from systems, networks and any other devices by individuals or systems.
Control Description	2.9.1 Data leakage prevention measures should be implemented to systems, networks, and any other devices that process, store, or transmit sensitive information, including, but not limited to, monitoring and following up on the transfer, copying, and extracting of sensitive data from systems and networks, such as emails and various storage media. Records of these processes should be retained, maintained, reviewed and periodically checked.
Control No./Name	2.10 Protection of Information Systems during Audit Tests
Purpose	To reduce the impact of auditing and other relevant activities on operating systems and business requirements.

Control Description	2.10.1 Audit tests and relevant activities, including operating systems assessment, should be planned and agreed upon by the auditor and the competent management.
Control No./Name	2.11 Testing Information
Purpose	To ensure the selection of the appropriate information for testing and protection of operational information used in testing.
Control Description	2.11.1 Testing information should be appropriately selected, protected, and managed.

3. Human Resources Security

Control No./Name	3.1 Background Screening
Purpose	To ensure that all employees are qualified and eligible for the roles they are nominated to undertake.
Control Description	3.1.2 Background checks for all job candidates (Screening) should be carried out before joining the entity and on an ongoing basis, taking into account the applicable laws, regulations and ethics and as per business requirements, the classification of information to be accessed and anticipated risks. 3.1.3 The entity should set the procedures and criteria for the screening of employees; these procedures should be periodically reviewed.
Control No./Name	3.2 Employment Terms and Conditions
Purpose	To ensure that employees are aware of the cybersecurity responsibilities for the roles assigned to them.
Control Description	3.2.2 The cybersecurity-related duties and obligations of the employees and the entity must be incorporated in the employment contracts that should include, as a minimum, the following: 1. The personnel responsibilities for the protection of the confidentiality of the entity's information that should not be disclosed.

	2. The legal and administrative responsibilities regarding intellectual property rights. 3. The responsibilities related to data protection, integrity and availability. 4. The responsibilities related to the classification and management of the entity's information. 5. The disciplinary process to be imposed in case any employee fails to fulfill the cybersecurity requirements. 3.2.3 The cybersecurity-related roles and responsibilities should be communicated to candidates during the pre-employment process. 3.2.4 The terms and Conditions related to cybersecurity should be reviewed when the applicable laws, regulations, cybersecurity policy or topic-specific policies are changed.
Control No./Name	3.3 Cybersecurity Awareness and Training
Purpose	To ensure that the employees and other interested parties are aware of and abide by their cybersecurity duties and responsibilities.
Control Description	3.3.2 Employees and interested parties should be provided with the proper cybersecurity training and education; they should be also provided with any updates of the entity's applicable cybersecurity policy and the topic-specific policies and procedures as required. 3.3.3 The entity should develop an awareness-raising program that aims to boost the employees' awareness of their cybersecurity-related responsibilities and the means that enable them to carry out these responsibilities. 3.3.4 The entity should identify, prepare and implement an appropriate cybersecurity training plan for the technical team whose roles require a specific set of skills and expertise.
Control No./Name	3.4 Disciplinary Process
Purpose	To ensure that employees and other interested parties are aware of the repercussions of violating Cybersecurity Policy, and that they are deterred and properly dealt with in case they commit such violations.
Control Description	3.4.1 The entity should develop a regulation of penalties (Disciplinary Process) to take actions against employees and other relevant parties as a repercussion of their violation of the Cybersecurity Policy.

Control No./Name	3.5 Responsibilities After Employee Termination or Change of Employment
Purpose	To protect the interests of the entity as part of the process of changing or terminating employment or contract.
Control Description	3.5.1 The cybersecurity responsibilities and duties that remain effective after contract termination or change of employment should be identified, enforced and communicated to employees concerned and other interested parties. 3.5.2 The responsibilities and duties that remain effective after contract termination or change of employment should be determined and stipulated in the terms and conditions of individuals employment, contracts or agreements, provided that the responsibilities include, as a minimum, maintaining the confidentiality of information and intellectual property rights.
Control No./Name	3.6 Non-Disclosure Agreements
Purpose	To ensure maintaining the confidentiality of information accessible by employees or external parties.
Control Description	3.6.1 Non-disclosure agreements that reflect the entity's requirements for information protection should be identified, documented, regularly reviewed, and signed by employees and other interested parties.

Protect 2

4 Physical Security

Control No./Name	4.1 Physical Security Perimeters
Purpose	To prevent unauthorized physical access, damage, and interference to the entity's information and other associated assets.
Control Description	4.1.1 The physical security perimeters (Physical Security) of information and other associated assets should be identified, documented, and protected.
Control No./Name	**4.2 Physical Entry**
Purpose	To ensure only authorized physical access to the entity's information and other associated assets.
Control Description	4.2.1 The physical security perimeters of information and assets should be protected by the appropriate cybersecurity controls of entry and access points, taking into consideration, as a minimum, the following: 1. Restricting access to the entity's sites and buildings to authorized employees only. 2. Ensuring that the management of access rights to physical areas include the periodical review, update and removal of access authorizations. 3. Maintaining, securely monitoring and protecting a physical logbook or an electronic audit log of all physical accesses. 4. Establishing the physical security measures to ensure the security of information and associated assets. 5. Managing the visitors' authorizations to enter sites and buildings. 6. Managing areas of loading and unloading for incoming materials relating to sites or buildings, ensuring their security checks to prevent unauthorized entry.
Control No./Name	**4.3 Protecting Offices, Rooms and Facilities**
Purpose	To prevent unauthorized physical access, damage, and interference to the entity's information and other associated assets in offices, rooms, and facilities.
Control Description	4.3.1 The physical security of offices, rooms and facilities should be designed and implemented.

Control No./Name	4.4 Physical Security Monitoring
Purpose	To detect and prevent unauthorized physical access.
Control Description	4.4.1 The buildings and premises should be continuously monitored for unauthorized physical access. 4.4.2 The buildings and premises should be monitored by video monitoring and surveillance systems such as closed-circuit television (CCTV) and physical security management software, either managed internally or by a monitoring service provider. 4.4.3 Surveillance systems should be protected from unauthorized access. 4.4.4 The period of retention of monitoring system logs and recorded videos should be determined as per the applicable laws and regulations. 4.4.5 Any monitoring and recording mechanism should be used as per the applicable laws and regulations, including data and personal identification information (PII) protection legislations, particularly concerning the monitoring of individuals and the retention periods of recorded videos.
Control No./Name	4.5 Protection Against Physical and Environmental Threats
Purpose	To prevent or reduce the repercussions of events arising from physical and environmental threats.
Control Description	4.5.1 Requirements for protection from physical and environmental threats, such as natural disasters and other intentional or unintentional physical threats to infrastructure should be designed and implemented. This should include, but not limited to the following: 1. Installing and configuring systems able to detect fire at an early stage by sending alarms or triggering fire suppression systems. 2. Adopting systems able to secure systems against electric surges or any similar events in order to minimize the repercussions. 3. Maintaining levels of environmental controls set by the entity inside the facilities, such as temperature, humidity, pressure or radiation. 4. Protecting systems from damage due to water leakage by providing master or isolation shutoff valves that are accessible and appropriately operating.

Control No./Name	4.6 Working in Secure Areas
Purpose	To protect information and other associated assets in secure area against damage and unauthorized interference by personnel working in such areas.
Control Description	4.6.1 Security procedures for working in secure areas should be developed and implemented.
Control No./Name	**4.7 Clear Desk and Clear Screen**
Purpose	To reduce the risks of unauthorized access, loss and damage of information on desks, screens and in other accessible locations during and after normal business hours.
Control Description	4.7.1 The entity should develop the Clear Desk and Clear Screen Policy that will include, as a minimum, the following: 1. Keeping the employee's office free from any paper business information that might cause data disclosure. 2. Leaving user devices logged off or secured with screen lock. 3. Safely storing documents and removable storage media (Removable Devices) that contain sensitive information, or securely disposing thereof when no longer needed.
Control No./Name	**4.8 Equipment Siting and Protection**
Purpose	To reduce risks from physical and environmental threats, unauthorized access, and damage.
Control Description	4.8.1 The equipment should be put in a safe and secured place.
Control No./Name	**4.9 Protection of Assets Off-Site**
Purpose	To prevent loss, damage, theft or compromise of off-site devices and avoiding disruption of the entity’s operations.
Control Description	4.9.1 The security of assets off-premises should be maintained

Control No./Name	4.10 Storage Media
Purpose	To ensure only authorized disclosure, modification, removal or destruction of information on storage media.
Control Description	4.10.1 The entity should develop a policy on managing removable storage media, that should be communicated to all relevant parties and should include, as a minimum, the following: 1. Managing and protecting the entity's information on storage media, that include paper documents, during their acquisition, use, transportation and disposal as per the cybersecurity requirements. 2. Encrypting the storage media if the information is highly confidential and its integrity is required. 3. Transferring the stored information to modern storage media to reduce the risks of Storage Media Degradation before becoming unreadable.
Control No./Name	4.11 Supporting Facilities
Purpose	To prevent loss, destruction or damage of information and other associated assets, or disruption of the entity’s services due to failure and disruption of supporting facilities.
Control Description	4.11.1 Information processing facilities should be protected from power outages and other disruptions caused by failures in supporting facilities such as electricity, telecommunications, water supply, gas, sewage, ventilation and air conditioning.
Control No./Name	4.12 Cabling Security
Purpose	To prevent the loss, damage, theft, or destruction of information and other associated assets and disruption of the entity’s services related to power and communications cables.
Control Description	4.12.1 Cables that carry power, data or supporting information services should be protected from interception, interference or damage.

Control No./Name	4.13 Equipment Maintenance
Purpose	To prevent loss, damage, theft, or destruction of information and other associated assets, and disruption of the entity’s services due to non-performance of the required maintenance.
Control Description	4.13.1 Equipment should be appropriately maintained to ensure information availability, integrity and confidentiality.

Control No./Name	4.14 The Secure Disposal or Reuse of Equipment
Purpose	To prevent any leakage of information from the equipment that will be disposed or reused.
Control Description	4.14.1 The components of equipment containing storage media should be checked well to verify that any sensitive data and licensed software have been removed or safely overwritten before disposal or reuse.

Protect 2

5. Secure Configurations

Control No./Name	5.1 Configuration Management
Purpose	To ensure that hardware, software, services, and networks are functioning properly with required security settings, and that configurations are not modified in an unauthorized or improper manner.
Control Description	5.1.1 The entity should determine, document and implement processes and use suitable tools to enforce configurations on hardware, software, services and networks as per cybersecurity requirements. 5.1.2 The entity should develop and periodically review templates and instructions for secure configurations (Configurations Templates) as per the applicable policies. 5.1.3 The entity should analyze any modification in configurations carried out to systems to determine the possible impacts on security and privacy prior to modification implementation. 5.1.4 The hardware, software, service and network configurations should be monitored and recorded. These records should be securely stored and periodically reviewed.
Control No./Name	5.2 The Usage of Cryptography
Purpose	To ensure the appropriate and effective use of cryptography to protect information confidentiality or integrity in accordance with business requirements and information security, taking into consideration the legal, legislative, regulatory and contractual requirements relating to cryptography.
Control Description	5.2.1 The rules for the effective use of cryptography, including the cryptographic keys management and protection, should be determined and implemented. 5.2.2 The entity should develop its Policy on Cryptography that should be communicated to all interested parties.

Protect 2

6. Networks and Systems Security

Control No./Name	6.1 Networks Security
Purpose	To protect information in networks and supporting information processing facilities from compromise via the network.
Control Description	6.1.1 Networks and network devices should be secured, managed, and controlled to protect information in systems and applications. 6.1.2 The entity should document network diagrams, and configurations of devices settings (such as switches and routers); they should be updated regularly. 6.1.3 The entity should properly record and monitor network activities to enable the detection of actions that might affect cybersecurity.
Control No./Name	6.2 The Security of Network Services
Purpose	To ensure the secure use of network services.
Control Description	6.2.1 The secure usage mechanisms, levels and requirements for network services should be determined, implemented and monitored (e.g., authentication and cryptography of network services).
Control No./Name	6.3 Segregation of Networks
Purpose	To split the networks and control traffic between them as per business needs and cybersecurity requirements.
Control Description	6.3.1 The groups of information services, users, information systems should be segregated and determined in the entity's networks. 6.3.2 The entity's internal networks should be segregated from the external networks.

Control No./Name	6.4 Working Remotely
Purpose	To ensure the security of information when the employees are working remotely.
Control Description	6.4.1 The security measures should be implemented to protect information that is accessed, processed or stored when employees are working remotely. 6.4.2 The entity should develop a topic-specific Remote Working Policy to ensure information security; it should include, as a minimum, the following: 1. The employee's commitment to comply with the cybersecurity requirements concerning the sensitivity of information, systems and applications; 2. The implementation of security measures, such as firewalls and protection against malware. 3. Audit and security monitoring.
Control No./Name	6.5 Web Filtering
Purpose	To protect systems against compromise due to browsing unauthorized web resources or downloading malware from them.
Control Description	6.5.1 Accessing external websites should be well managed (Web Filtering) by using appropriate techniques to reduce exposure to malicious content.
Control No./Name	6.6 Separation of Development, Testing and Production Environments
Purpose	To protect the production environment and data against compromise by separating development, testing and production environments.
Control Description	6.6.1 The development, testing, and production environments must be separated and secured. 6.6.2 Changes should be analyzed in a separate testing environment before implementing an operational environment to ensure the compliance of changes with the cybersecurity requirements.

Control No./Name	6.7 Change Management
Purpose	To preserve information security when implementing changes.
Control Description	6.7.1 Changes made to information processing facilities and information systems should be subject to change management measures. 6.7.2 The entity should identify, document and approve changes made to systems and enforce restrict physical and logical access associated with these changes.

Control No./Name	6.8 Wireless Networks Protection
Purpose	To ensure the secure usage of wireless networks to preserve information security.
Control Description	6.8.1 Wireless networks should be secured by using safe means of identity verification and encryption, and separating wireless networks from the entity's internal network. They should not be connected unless a comprehensive study of the arising risks is made, and it is ensured that they are handled in a way that maintains the protection of the entity's technical assets.

Protect 2

7. Applications Security

Control No./Name	7.1 Installation of Software on Operational Systems
Purpose	To ensure the integrity of operational systems and prevent the exploitation of known (publicly disclosed) technical vulnerabilities related to installed software.
Control Description	7.1.1 The procedures and measures must be implemented to safely manage software installation on operational systems. 7.1.2 The software patches and updates should be implemented that help remove or reduce information security vulnerabilities. 7.1.3 The entity should keep audit logs for all software updates.
Control No./Name	7.2 The Use of Privileged Utility Programs
Purpose	To ensure the use of privileged utility programs as per cybersecurity requirements.
Control Description	7.2.1 The use of privileged utility programs that may be able to override system and application controls should be firmly restricted and monitored.
Control No./Name	7.3 The Safe Development Life Cycle of Software
Purpose	To ensure the cybersecurity requirements are designed and implemented in the safe development life cycle of software and systems.

Control Description	7.3.1 The rules for the safe development of software and systems should be developed and implemented; they should include, as a minimum, the following: 1 The guidelines of safe programming for each programming language used. 2 The cybersecurity requirements and technical specifications and designs that should be clearly determined and achieved. 3 The cybersecurity tests, including but not limited to code review and penetration testing. 4 Safe repositories that all codes should be kept securely therein, and ensuring that configurations of the source code repositories are set as per cybersecurity requirements.
Control No./Name	7.4 Applications Cybersecurity Requirements
Purpose	To ensure that all cybersecurity requirements are identified and satisfied when developing or acquiring applications.
Control Description	7.4.1 Cybersecurity requirements should be identified and agreed upon when developing or acquiring applications through the relevant risk assessments. These requirements should include, but not be limited to: 1. Security and privacy requirements. 2. A description of the operational environment for applications in a way that ensures they are properly functioning. 3. The criteria for fulfilling these requirements.
Control No./Name	7.5 Secure Coding
Purpose	To ensure that the software is written securely, thus reducing the number of potential technical security vulnerabilities in the software.
Control Description	7.5.1 The secure coding rules and processes should be implemented throughout the software development life cycle.
Control No./Name	7.6 Securing System Architecture and Engineering Principles
Purpose	To ensure information systems are securely designed, implemented throughout the development life cycle.
Control Description	7.6.1 The principles of engineering secure systems should be developed, documented, maintained and applied to any information systems development activities, including but not limited to: 1. “Secure by design” 2. “Defense in Depth” 3. “Secure by default” 4. “Deny by default” 5. “Always assume breach” 6. “Least Privileges Principle”

Control No./Name	7.7 Cybersecurity Testing in Applications Development and Acceptance
Purpose	To ensure that cybersecurity requirements are fulfilled when applications or codes are deployed and released in the production environment.
Control Description	7.7.1 The cybersecurity testing processes should be determined and implemented throughout the development life cycle; the test results should be documented.
Control No./Name	**7.8 Penetration Tests**
Purpose	To ensure that vulnerabilities in the entity's systems are identified and addressed to thwart attackers attempts to exploit them.
Control Description	7.8.1 The entity should periodically conduct and document penetration tests. 7.8.2 The entity should periodically conduct a review process to ensure that the cybersecurity requirements for penetration testing processes are fulfilled and implemented.
Control No./Name	**7.9 Web Applications Security**
Purpose	To reduce cybersecurity risks and threats that target web applications.
Control Description	7.9.1 The entity's external web applications should be protected from cyber risks by determining, documenting and approving cybersecurity requirements. 7.9.2 Cybersecurity requirements should be implemented to protect the entity's external web applications. 7.9.3 The cybersecurity requirements for protecting the entity's external web applications should include, as a minimum, the following: 1. The usage of a Web Application Firewall. 2. The usage of the "Multi-tier Architecture" principle. 3. The usage of security protocols (such as HTTPS). 4. Clarification of the Users' Acceptable and Safe Usage Policy. 5. The usage of Multi-Factor Authentication to secure users' login process. 7.9.4 The cybersecurity requirements for protecting the entity's web applications from cyber risks should be periodically reviewed.

Detect 3

1. Threats and vulnerabilities Management	
Control No./Name	1.1 Technical Vulnerabilities Management
Purpose	To revent exploitation of technical vulnerabilities.

Control Description	1.1.1 The technical vulnerabilities management processes should be developed and documented, taking into consideration, as a minimum, the following: 1. Obtaining information about technical vulnerability as per the entity's list of assets. 2. Determining and monitoring technical vulnerabilities as per the entity's list of assets. 3. Conducting analysis, verification, address and documentation of reports regarding technical vulnerabilities and taking appropriate Correction actions. 4. Developing a plan for technical vulnerabilities scanning and penetration testing, ensuring that it is periodically implemented.
Control No./Name	1.2 Threat Intelligence Information
Purpose	To provide awareness of the organization's threat environment so that the appropriate mitigation actions can be taken.
Control Description	1.2.1 Information related to cybersecurity threats should be collected and analyzed to obtain Threat Intelligence Information to be able to encounter and address these threats. 1.2.2 The entity should use such information to prevent, detect or respond to threats in order to minimize their impacts in case they affect the entity.

Detect 3

2.Cybersecurity Events Management

Control No./Name	2.1 Clock Synchronization
Purpose	To ensure the correlation and analysis of cybersecurity-related events and other recorded data, and supporting investigations into cybersecurity incidents.
Control Description	2.1.1 The clocks of the information processing systems used by the entity should be synchronized (Clock Synchronization) with the approved time sources. 2.1.2 The entity should determine a standard reference time to be used within the entity for all systems, including building management systems, entry and exit systems, and other systems that can be used to aid in investigations.
Control No./Name	**2.2 Reporting (Suspected) Cybersecurity Events**
Purpose	To support the timely, consistent and effective reporting of (suspected) cybersecurity events identified by personnel.
Control Description	2.2.1 The entity should develop a mechanism for its personnel to report observed or suspected cybersecurity events upon their occurrence. 2.2.2 The entity should review and follow up on these reports to take the appropriate actions to analyze, verify, respond to and process them.
Control No./Name	**2.3 Logging**
Purpose	To record events to ensure the integrity of log information. prevent against unauthorized access, identify Cybersecurity events that can lead to a Cybersecurity incident and to support investigations.
Control Description	2.3.1 Logs that record activities, exceptions, failures, and other relevant events should be created, stored, protected, and analyzed. 2.3.2 The entity should keep audit logs for a certain period of time to be determined by the entity for administrative, legal, auditing or other operational purposes, until it is determined that such records are no longer needed.
Control No./Name	**2.4 Monitoring Activities**
Purpose	To detect anomalous behavior and potential cybersecurity incidents.

Control Description	2.4.1 Networks, systems and applications should be monitored to detect any anomalous behavior and take appropriate measures to assess potential cybersecurity incidents. 2.4.2 Unusual events should be reported to concerned parties to enhance cybersecurity auditing and assessment activities, and to handle and detect security vulnerabilities.

Respond 4


Respond
Taking the Required Measures to Encounter Cyber Incidents and Threats.

1. Incident Management

Control No./Name	1.1 Planning and Preparing for Cybersecurity Incident Management
Purpose	To ensure an immediate, effective and well-ordered response to cybersecurity incidents, including communication concerning cybersecurity incidents.
Control Description	1.1 The entity should plan and make needed preparations for cybersecurity incident management by determining and developing cybersecurity incident management processes and procedures, and all relevant roles and responsibilities. 1.2 The procedures for cybersecurity incident management should include, as a minimum, the following: 1. A mechanism for reporting cybersecurity incidents; it should include the point of contact. 2. The actions that should be taken in case a cybersecurity incident occurs. 3. Employees should be required to report suspected incidents within a definite period of time to be determined by the entity. 4. Reporting templates and forms for reporting cybersecurity incidents to support personnel in taking all required measures. 5. Logs and audit records that should be kept for a period of time to be determined by the entity to support personnel in carrying out post-incident investigations. 6. Incident Documentation: Comprehensive documentation of incident details, actions taken, and outcomes.
Control No./Name	1.2 Assessing and Deciding on Cybersecurity Events
Purpose	To ensure the effective and efficient response of cybersecurity events.
Control Description	1.2.1 The entity should assess the cybersecurity events and decide if they will be categorized as cybersecurity incidents. 1.2.2 The results of assessment and decision should be recorded in detail to be used as a reference, and evidence and to be used in the future. 1.2.3 Continues improvement Regularly update and improve your incident response plan based on lessons learned from previous incidents and changes in the threat landscape.

Control No./Name	1.3 Cybersecurity Incidents Response
Purpose	To ensure effective management of evidence response to cybersecurity incidents.
Control Description	1.3.1 Cybersecurity Incidents Response should take place as per the documented procedures, that include, as a minimum, the following: 1. Collecting and maintaining relevant evidence and records. 2. Post-incident analysis to identify the root cause of the incident. It should be ensured that it is documented and communicated to request countermeasures to encounter it. 3. Containing and controlling the cybersecurity incident. 4. Identifying and managing the vulnerabilities and shortcomings that caused the incident, contributed to its occurrence, or failed to thwart it.
Control No./Name	1.4 Collecting Evidence
Purpose	To ensure the management of the process of collecting evidence related to cybersecurity incidents for disciplinary and legal purposes.
Control Description	1.4.1 The entity should develop and implement procedures to identify, collect and obtain evidence related to cybersecurity incidents as per the types of storage media, devices and the device status.
Control No./Name	1.5 Learning from Cybersecurity Incidents
Purpose	To reduce the likelihood or repercussions of future incidents.
Control Description	1.5.1 The knowledge gained from cybersecurity incidents should be used to improve and develop cybersecurity controls through training, testing and conducting awareness sessions. 1.5.2 The entity should make use of the lessons learned from cyber incident response activities: the procedures and measures taken, training provided, testing conducted and awareness sessions provided, in addition to the implementation of the needed changes.

Recovery

Recovery

Developing and Implementing the Appropriate Activities Required to Maintain Resilience Plans and Recover any Capabilities or Services that have been Hampered due to Cybersecurity Incidents.

1. Continuity

Control No./Name	1.1 Information Backup
Purpose	To enable recovery from loss of data or systems.
Control Description	1.1.1 Backups of information, software and systems should be kept, maintained and regularly tested as per the applicable and approved topic-specific Policy on Backup and put schedule for data backup. 1.1.2 Backup copies should be protected by encryption as per specific risks and according to the degree to which confidentiality is required. 1.1.3 The operational procedures for implementing and scheduling backups and dealing with failures should be monitored to ensure completeness of backups as per the relevant topic-specific policy. 1.1.4 Backups should be stored in a secure place remote from their main location to restore business activities in case an accident or a natural disaster occurs. 1.1.5 Systems backup procedures should be regularly tested to ensure their efficiency and that they fulfill the incident response objectives and business continuity plans; they should include restoration and recovery time tests. 1.1.6 The duration of backup copies retention should be determined.
Control No./Name	1.2 Cybersecurity during Disruptions
Purpose	To protect information and other associated assets during disruptions.
Control Description	1.2.1 The entity should plan how to fulfill and maintain cybersecurity requirements at a proper level during disruptions.
Control No./Name	1.3 ICT Readiness for Business Continuity
Purpose	To ensure the availability of information and other associated assets during disruptions.
Control Description	1.3.1 ICT readiness should be planned, implemented, maintained and tested as per business continuity objectives and ICT continuity requirements. 1.3.2 The entity should identify and provide ICT continuity requirements and set priorities according to the Business Impact Analysis

Recovery

2. Cybersecurity Resilience

Control No./Name	2.1 Cyber Resilience Management
Purpose	To ensure the ability to recover from cyber incidents and disasters
Control Description	2.1.1 The entity should develop plans that may affect the entity's business continuity. 2.1.2 Disaster recovery plans should be established.

Terminologies and Definitions

Table (2) below mentions the most significant terminologies and their definitions set forth in the Essential Controls herein.

Table 2 - Terminologies and Definitions

Terminology	Definition
Cybersecurity	Refers to the set of policies, guidelines, security concepts, risk management approaches, procedures, and technologies that could be used to protect the entity's assets, including the protection of networks and information technology systems. “Cybersecurity” comprises information security, electronic security, and digital security.
Cybersecurity Policy	Refers to the set of rules and directives that aim to protect networks, information technology systems, and other assets in entity to maintain the confidentiality, integrity, and availability of information.
Topic-Specific Polices	Refers to the rules and directives relating to a topic-specific subject; they are set by the top management in the entity.
Process	Refers to a set of correlated and interactive activities used to change inputs into outputs and outcomes.
Procedure	Refers to the detailed description of the steps required to perform specific operations or activities that comply with the relevant standards and policies. Procedures are defined as part of the processes.
Identify	Refers to the development of the regulatory insight into managing cybersecurity risks that target systems and assets.
Protect	Refers to the enhancement of entities’ capabilities and the development of the security measures needed to protect systems and assets.
Detect	Refers to the development and implementation of appropriate activities needed to detect suspected events and cyber threats.
Respond	Refers to the necessary measures and steps needed to combat cyber incidents and threats.
Recovery	Refers to the development and implementation of appropriate activities to maintain resilience plans and recover any capabilities or services that have been disrupted due to the occurrence of cybersecurity incidents.

Governance	Refers to the set of rules and essentials that organize work in an entity, maintain effective control over its management system, and regulate the relationship between it and stakeholders.
Asset	Refers to the properties, resources or items that the entity owns and has a value to the entity. It includes individuals, services, hardware, software, information and other items.
Denial of Service (DoS) Attacks	Refers to an attack that aims to make users unable to use the service, as the perpetrator exploits the vulnerabilities in the structure of the system attacked in order to disrupt the service.
Outsourced Development	Refers to the obtainment of services or goods by contracting with a supplier or an external service provider.
Audit	Refers to the independent review and checking of the entity's records and activities, and issuance of recommendations for taking any necessary changes to test the extent of adequacy and efficacy of cybersecurity controls and ensure compliance with the applicable operational policies and procedures.
Audit Logs	Refers to the aggregated data that might be used to facilitate security auditing.
Confidentiality	Refers to the obligation to maintain the protection of data and information from unauthorized access.
Integrity	Refers to the process that ensures data accuracy and intactness and that they have not been altered or damaged in an unauthorized way.
Availability	Refers to the ability to ensure that the essential data, services and resources related to systems and applications are available to users whenever required.
Privacy	Refers to the individuals' right to control or affect the handling or disclosure of relevant information relating to them.
Personal Identifiable Information (PII) Protection	Refers to the method of verifying the identity of a user, process, or service; it is an essential method required for granting access to the entity's resources.
Segregation of Duties	Refers to the principle that is based on separating conflicting duties and responsibilities between different individuals to stop any individual from carrying out his/her duties individually and with different privileges.
Privileged access	Refers to the process of management of high-risk privileges on the entity's systems; they often require special handling to minimize risks that might arise from their misuse.
Least Privilege Principle	Refers to the principle of granting users and processes the minimal level of access to be able to carry out their specific tasks or functions in order to limit potential harms.

Security By Design	Refers to the process that ensures that the software and applications have been designed to be functionally secure in principle, and that security has been prioritized and incorporated into the system in all components and configurations.
Defense In Depth	Refers to the strategy that aims to strengthen the level of protection of systems, data and information stored therein by employing several layers of protection. These layers include the implementation of various protection measures at different levels, such as networks, hardware, software, data, in addition to the regulation of access to resources and other assets.
Disaster Recovery Plan	Refers to a documented and structured approach that outlines the steps and procedures required to recover and restore critical IT systems, applications, and data to their previous or alternate state after the occurrence of a sudden event such as a natural disaster, cyber-attack, or system failure. This plan comprises identifying critical systems and data, backup, recovery procedures, and the communication protocols required to report measures to employees and customers in addition to the recovery time objective (RTO) and recovery point objective (RPO) requirements. A Disaster Recovery Plan is essential to minimize the impact of a power failure on the entity's operations, reputation, and financial status. It should be periodically reviewed, updated, and tested to ensure its efficacy.
Intellectual Property Rights	Refers to the rights that protect information and digital assets created, used, and circulated over the Internet, networks, and other electronic systems in order to secure digital assets and sensitive information from compromise, theft, and illegal use.
Phishing Emails	Refers to the emails used to deceive users into obtaining sensitive information from them. Attackers typically send phishing emails; as they fake email addresses to steal information or push recipients to download malware, thereby they gain unauthorized access to their devices.
Spam Emails	Refers to emails that contain irritating marketing and advertisements. These unsolicited emails are sent in bulk and are not directed to a huge number of people. Such emails might contain insecure links or direct recipient to web pages used to steal personal information; thus they pose great risk to the cybersecurity of individuals and entities.