



الهيئة الوطنية
للأمن السيبراني
National Cybersecurity Authority

Essential Cybersecurity Controls

(ECC – 2: 2024)

TLP: White

Document Classification: **Public**

Disclaimer: Please refer to the National Cybersecurity Authority's website (<https://nca.gov.sa>), to obtain the latest version of this document.

In the Name of Allah,
The Most Gracious,
The Most Merciful

Disclaimer: The following controls will be governed by and implemented in accordance with the laws of the Kingdom of Saudi Arabia, and must be subject to the exclusive jurisdiction of the courts of the Kingdom of Saudi Arabia. Therefore, the Arabic version will be the binding language for all matters relating to the meaning or interoperation of this document.

Traffic Light Protocol (TLP):

This marking protocol is widely used around the world to share sensitive data. It has four colors (traffic lights):



Red – Personal and Confidential to the Recipient Only

The recipient has no rights to share information classified in red with any person outside the defined range of recipients, either inside or outside the entity.



Amber – Restricted Sharing

The recipient may share information marked in amber with the concerned personnel only within the same entity, and with those required to take action with regard to the information.



Green – Sharing within the Same Community

The recipient may share information marked in green with other recipients inside the same entity or with others in a related entity or in an entity within the same sector. However, sharing or publishing this information on public platforms is not permitted.



White – No Restrictions

Update and Review

NCA will periodically review and update the ECC as per the cybersecurity requirements and related industry updates. NCA will communicate and publish the updated version of ECC for implementation and compliance. NCA has updated the previous version of the ECC (i.e., ECC-1:2018).

Version	Year of Issuance	Updates
ECC – 1	2018	-
ECC – 2	2024	Appendix (C) illustrates the updates on the previous version

Table of Contents

Update and Review	3
Introduction.....	7
Objectives	8
Scope of Work and Applicability	9
ECC Scope of Work	9
ECC Statement of Applicability	9
Implementation and Compliance	9
Assessment and Compliance Tool	9
ECC Domains and Structure	10
Main Domains	10
Subdomains	11
Structure	12
The Essential Cybersecurity Controls (ECC).....	13
Details of the Essential Cybersecurity Controls (ECC)	13
Cybersecurity Governance	13
Cybersecurity Defense.....	19
Cybersecurity Resilience	29
Third-Party and Cloud Computing Cybersecurity.....	30
Appendices.....	32
Appendix (A): Terms and Definitions	32
Appendix (B): List of the Abbreviations	41
Appendix (C): List of Updates	42

List of Tables

Table 1 Document Versions.....	13
Table 2: ECC Structure	16
table 3 Terms and Definition	53
Table 4 List of Abbreviations.....	54

List of Figures

Figure 1: Main Domains of ECC.....	14
Figure 2: ECC Subdomains	15
Figure 3: Controls Coding scheme	16
Figure 4: ECC Structure	16

Executive Summary

The Kingdom of Saudi Arabia's Vision 2030 aims for a comprehensive improvement of the nation and its security, economy, and citizens' well-being and decent life. Naturally, one of the essential goals of Vision 2030 is the transformation towards digitalization and the improvement of digital infrastructure, in order to keep up with the accelerated global progress in digital services, renewable global networks, IT systems, and OT systems, align with growing computer processing and massive data storage and exchange capabilities, and be prepared for handling artificial intelligence and the fourth 4th industrial revolution transformations.

This transformation requires streamlining the flow of information, securing it, and preserving the integration of all systems. It also requires maintaining and supporting the cybersecurity of the Kingdom, in order to protect the State's vital interests, national security, critical infrastructures, high priority sectors, and governmental services and activities. To this end, the National Cybersecurity Authority (NCA) was established, and the NCA's Statute was approved by Royal Order No. 6801, dated 11/02/1439H., making the NCA the national and specialized cybersecurity reference in the Kingdom.

NCA's powers and duties fulfill the strategic cybersecurity needs and the need to develop cybersecurity policies, governance mechanisms, frameworks, standards, controls, and guidelines, and disseminate them across entities.

NCA's powers and duties also fulfil the needs of updating and continuously monitoring the compliance of government agencies and non-government entities, as the role and significance of cybersecurity have significantly increased more than ever with the rise of security risks in the cyberspace.

NCA's Statute states that no public agency, private entity, or any other entity shall be relieved from their responsibility towards their own cybersecurity, as confirmed by High Order No. 57231, dated 10/11/1439H., which states that "all government agencies must raise the level of their cybersecurity to protect their electronic networks, systems and data, and to abide by the NCA's policies, frameworks, standards, controls, and guidelines in this regard".

From this perspective, the NCA has developed the Essential Cybersecurity Controls (ECC-1: 2018) to set the minimum cybersecurity requirements for national entities falling within the ECC scope of work. This document outlines the details, goals, scope of work, applicability, and compliance and monitoring mechanism of the ECC.

All national entities shall take the necessary measures to ensure ongoing and continuous compliance with the ECC, as per Article 10(3) of the NCA's Statute and High Order No. 57231, dated 10/11/1439H.

Introduction

The National Cybersecurity Authority (Hereinafter referred to as the “NCA”) developed the Essential Cybersecurity Controls (ECC–1:2018) after conducting a study on multiple cybersecurity standards, frameworks, and controls that have previously been developed by (national and international) entities and organizations, considering the requirements of relevant national legislations, regulations, and decisions, as well as reviewing and leveraging cybersecurity best practices, analyzing previous cybersecurity incidents and attacks against government agencies and other critical entities, and surveying and considering opinions of multiple national entities.

The Essential Cybersecurity Controls consist of the following:

- 4 Cybersecurity Main Domains.
- 28 Cybersecurity Subdomains.
- 108 Cybersecurity Main Controls.
- 92 Cybersecurity Subcontrols.

Moreover, these Controls are linked to relevant national and international legislative and regulatory requirements.

Objectives

These Controls aim to provide the minimum cybersecurity requirements based on the best practices and standards to minimize the internal and external cybersecurity threats against the entities' information and technology assets. The protection of the entity's information and technology assets requires focusing on the key protection goals, which are as follows:

- Confidentiality
- Integrity
- Availability

These Controls take into account the following four main cybersecurity pillars:

- Strategy
- People
- Process
- Technology

Scope of Work and Applicability

ECC Scope of Work

These Controls are applicable to government agencies in the Kingdom of Saudi Arabia (including ministries, authorities, establishments and others) and their affiliated companies and entities (inside and outside the kingdom), as well as all private sector entities owning, operating, or hosting Critical National Infrastructures (CNIs) (Hereinafter referred to collectively as the "entity"). The NCA strongly encourages all other entities in the Kingdom to leverage these Controls to implement best practices to improve and enhance their cybersecurity.

ECC Statement of Applicability

These Controls have been developed to fulfill the cybersecurity needs of all entities and sectors in the Kingdom, taking into account the diverse nature of their businesses. Each entity shall comply with all controls applicable thereto.

Here are some examples of controls the applicability of which varies from one entity to another based on the entity's business and use of certain technologies:

- Controls under the Subdomain (4-2) relating to Cloud Computing and Hosting Cybersecurity are applicable and binding on entities currently using or planning to use cloud computing and hosting services.

Implementation and Compliance

As per Article 10(3) of the NCA's Statute and High Order No. 57231, dated 10/11/1439H., all entities within the scope of these Controls shall take all necessary measures to ensure ongoing and continuous compliance with these Controls.

The NCA shall evaluate the entities' compliance with the ECC through multiple means, such as self-assessment by the entities, periodic reports of the compliance tool, and/or field auditing visits, in accordance with the mechanism deemed appropriate by the NCA.

Assessment and Compliance Tool

The NCA will issue a tool (ECC-2:2024 Assessment and Compliance Tool) to organize the process of assessment and measurement of compliance by entities in applying the ECC.

ECC Domains and Structure

Main Domains

Figure (1) below shows the main domains of the ECC.



FIGURE 1: MAIN DOMAINS OF ECC

Subdomains

Figure (2) below shows the ECC subdomains

1. Cybersecurity Governance	1-1	Cybersecurity Strategy	1-2	Cybersecurity Management
	1-3	Cybersecurity Policies and Procedures	1-4	Cybersecurity Roles and Responsibilities
	1-5	Cybersecurity Risk Management	1-6	Cybersecurity in Information and Technology Project Management
	1-7	Compliance with Cybersecurity Standards, Laws and Regulations	1-8	Periodical Cybersecurity Review and Audit
	1-9	Cybersecurity in Human Resources	1-10	Cybersecurity Awareness and Training Program
2- Cybersecurity Defense	2-1	Asset Management	2-2	Identity and Access Management
	2-3	Information Systems and Information Processing Facilities Protection	2-4	Email Protection
	2-5	Network Security Management	2-6	Mobile Devices Security
	2-7	Data and Information Protection	2-8	Cryptography
	2-9	Backup and Recovery Management	2-10	Vulnerability Management
	2-11	Penetration Testing	2-12	Cybersecurity Event Logs and Monitoring Management
	2-13	Cybersecurity Incident and Threat Management	2-14	Physical Security
	2-15	Web Application Security		
3- Cybersecurity Resilience	3-1	Cybersecurity Resilience Aspects of Business Continuity Management (BCM)		
4- Third-Party and Cloud Computing Cybersecurity	4-1	Third-Party Cybersecurity	4-2	Cloud Computing and Hosting Cybersecurity

FIGURE 2: ECC SUBDOMAIN

Structure

Figures (3) and (4) below show the meaning of controls codes.

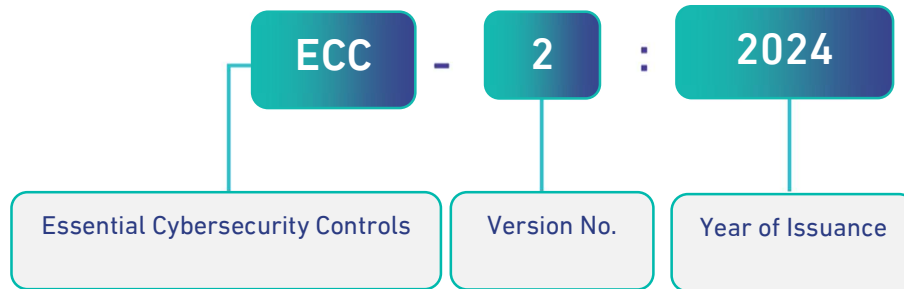


FIGURE 3: CONTROLS CODING SCHEME

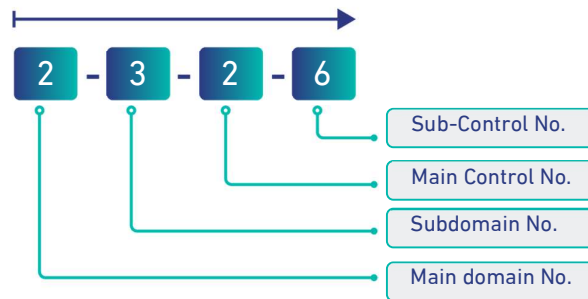


FIGURE 4: ECC STRUCTURE

Table (1) below shows the ECC methodological structure.

TABLE 1: ECC STRUCTURE

	Name of Main Domain
Reference Number of Main Domain	
Reference Number of Subdomain	Name of Subdomain
Objective	
Controls	
Control Reference Number	Control Clauses

The Essential Cybersecurity Controls (ECC)

Details of the Essential Cybersecurity Controls (ECC)

1 cybersecurity Governance

1-1	Cybersecurity Strategy
Objective	To ensure that the action plans, objectives, initiatives, and projects of the entity contribute to compliance with the relevant legislative and regulatory requirements.
Controls	
1-1-1	The cybersecurity strategy of the entity shall be identified, documented, and approved, and it shall be supported by the head of the entity or his/her delegate (Hereinafter referred to as the “Authorized Official”). The strategy goals shall be in line with the relevant legislative and regulatory requirements.
1-1-2	The entity shall execute an action plan to apply the cybersecurity strategy.
1-1-3	The cybersecurity strategy shall be reviewed at planned intervals (or in case of changes to the relevant legislative and regulatory requirements).
1-2	Cybersecurity Management
Objective	To ensure that the Authorized Official of the entity complies with and supports the implementation and management of cybersecurity programs within the entity, as per the relevant legislative and regulatory requirements.
Controls	
1-2-1	A department for cybersecurity shall be established within the entity. This department shall be independent from the Information Technology and Communications Department (As per High Order No. 37140, dated 14/08/1438H.). It is recommended that the Cybersecurity Department reports directly to the head of the entity or his/her delegate while ensuring that this does not result in a conflict of interests.
1-2-2	All cybersecurity positions shall be filled out with full-time and qualified Saudi cybersecurity professionals.
1-2-3	A cybersecurity supervisory committee shall be established pursuant to the instruction of the entity’s Authorized Official to ensure compliance with, support for, and monitoring of the implementation of the cybersecurity programs and regulations. The committee’s members, responsibilities, and governance framework shall be identified, documented, and approved. The committee shall include the head of the cybersecurity

	department as a member. It is recommended that the committee reports directly to the head of the entity or his/her delegate while ensuring that this does not result in a conflict of interests.
1-3	Cybersecurity Policies and Procedures
Objective	To ensure that the cybersecurity requirements and the entity's compliance therewith are documented and communicated, as per the entity's regulatory requirements and the relevant legislative and regulatory requirements.
Controls	
1-3-1	The cybersecurity department of the entity shall identify and document cybersecurity policies and procedures, including the cybersecurity controls and requirements, and have them approved by the entity's Authorized Official, and communicate them to the relevant personnel and parties inside the entity.
1-3-2	The cybersecurity department shall ensure that the cybersecurity policies and procedures, including the relevant controls and requirements, are implemented at the entity.
1-3-3	The cybersecurity policies and procedures shall be supported by technical security standards (e.g. technical security standards for firewall, databases, operating systems, etc.).
1-3-4	The cybersecurity policies and procedures shall be reviewed and updated at planned intervals (or in case of changes to the relevant legislative and regulatory requirements and standards). Changes shall be documented and approved.
1-4	Cybersecurity Roles and Responsibilities
Objective	To ensure that roles and responsibilities are clearly defined for all parties participating in implementing the cybersecurity controls within the entity.
Controls	
1-4-1	The Authorized Official shall identify, document, and approve the governance organizational structure, roles, and responsibilities of the entity's cybersecurity, and assign the persons concerned therewith. The necessary support shall be provided for the implementation thereof while ensuring that this does not result in a conflict of interests.
1-4-2	The cybersecurity roles and responsibilities within the entity shall be reviewed and updated at planned intervals (or in case of changes to the relevant legislative and regulatory requirements).

1-5	Cybersecurity Risk Management
Objective	To ensure managing cybersecurity risks in a methodological approach, in order to protect the entity's information and technology assets, as per the entity's regulatory policies and procedures and the relevant legislative and regulatory requirements.
Controls	
1-5-1	The cybersecurity department of the entity shall identify, document, and approve the cybersecurity risk management methodology and procedures within the entity, in accordance with considerations of confidentiality, and the integrity and availability of information and technology assets.
1-5-2	The cybersecurity department shall implement the cybersecurity risk management methodology and procedures within the entity.
1-5-3	The cybersecurity risk assessment procedures shall be implemented at least in the following cases: 1.5.3.1 At early stage of technology projects. 1.5.3.2 Before making major changes to technology infrastructure. 1.5.3.3 During planning to obtain third party services. 1.5.3.4 During planning and before the release of new technology services and products.
1-5-4	The cybersecurity risk management methodology and procedures shall be reviewed and updated at planned intervals (or in case of changes to the relevant legislative and regulatory requirements and standards). Changes shall be documented and approved.
1-6	Cybersecurity in Information and Technology Project Management
Objective	To ensure that cybersecurity requirements are included in the methodology and procedures of the entity's project management, in order to protect the confidentiality, integrity, accuracy, and availability of the entity's information and technology assets, as per the entity's regulatory policies and procedures and the relevant legislative and regulatory requirements.
Controls	
1-6-1	Cybersecurity requirements shall be included in the project management methodology and procedures and in the information and technology asset change management within the entity to ensure identifying and managing cybersecurity risks as part of the technology project lifecycle. The cybersecurity requirements shall be a key part of the requirements for technology projects.

1-6-2	The cybersecurity requirements for project management and information and technology asset changes within the entity shall include the following as a minimum: 1.6.2.1 Vulnerability assessment and remediation. 1.6.2.2 Reviewing secure configuration and hardening and updates packages before launching projects and changes.
1-6-3	The cybersecurity requirements for software and application development projects within the entity shall include the following as a minimum: 1.6.3.1 Using the secure coding standards. 1.6.3.2 Using trusted and licensed sources for software development tools and libraries. 1.6.3.3 Conducting compliance test for software against the cybersecurity requirements within the entity. 1.6.3.4 Secure integration between applications. 1.6.3.5 Reviewing secure configuration and hardening and updates packages before launching software products
1-6-4	The cybersecurity requirements for project management within the entity shall be periodically reviewed.
1.7	Compliance with Cybersecurity Standards, Laws and Regulations
Objective	To ensure that the entity's cybersecurity program complies with the relevant legislative and regulatory requirements.
Controls	
1-7-1	If there are nationally approved international agreements or commitments that include cybersecurity requirements, the entity shall identify and comply with these requirements.
1-8	Periodical Cybersecurity Review and Audit
Objective	To ensure that the cybersecurity controls adopted by the entity are implemented and applicable in accordance with the entity's regulatory policies and procedures, relevant national legislative and regulatory requirements, and international requirements imposed on the entity by law.
Controls	
1-8-1	The cybersecurity department of the entity shall periodically review the implementation of cybersecurity controls by the entity.

1-8-2	The implementation of cybersecurity controls by the entity shall be reviewed and audited by parties other than the cybersecurity department at the entity, provided that the audit and review are to be conducted independently while considering the principle of conflict of interest, as per the Generally Accepted Auditing Standards (GAAS) and the relevant legislative and regulatory requirements.
1-8-3	The results of cybersecurity audits and reviews shall be documented and presented to the cybersecurity supervisory committee and the Authorized Official. Results shall include the audit and review scope, observations, recommendations, corrective actions, and remediation plans.
1-9	Cybersecurity in Human Resources
Objective	To ensure that cybersecurity risks and requirements for personnel (employees and contractors) of the entity are managed efficiently prior to, during, and upon the end or termination of their employment, as per the entity's regulatory policies and procedures and the relevant legislative and regulatory requirements.
Controls	
1-9-1	Cybersecurity requirements for personnel of the entity shall be identified, documented, and approved prior to, during, and upon the end or termination of their employment.
1-9-2	Cybersecurity requirements for personnel of the entity shall be implemented.
1-9-3	Cybersecurity requirements prior to the commencement of the employment relationship between personnel and the entity shall include the following as a minimum: 1.9.3.1 Incorporating the personnel's cybersecurity responsibilities clauses and non-disclosure clauses in their employment contracts with the entity (including during and after employment end/termination with the entity). 1.9.3.2 Conducting screening or vetting for personnel in cybersecurity positions and technical positions with critical and privileged powers.
1-9-4	Cybersecurity requirements for personnel during their employment relationship with the entity shall include the following as a minimum: 1.9.4.1 Cybersecurity awareness (during on-boarding and during employment). 1.9.4.2 Implementation and compliance with cybersecurity requirements, as per the entity's cybersecurity policies, procedures, and operations.
1-9-5	The personnel's powers shall be reviewed and revoked immediately upon the end/termination of their employment with the entity.
1-9-6	Cybersecurity requirements for personnel of the entity shall be periodically reviewed.

1-10	Cybersecurity Awareness and Training Program
Objective	To ensure that the entity's personnel have the required security awareness, are aware of their cybersecurity responsibilities, and are equipped with the required cybersecurity skills, qualifications, and training courses in order to protect the entity's information and technology assets and fulfill their cybersecurity duties.
Controls	
1-10-1	A cybersecurity awareness program, delivered through multiple channels, shall be periodically developed and approved by the entity to strengthen the awareness about cybersecurity, cyber threats, and risks, and to build a positive cybersecurity awareness culture.
1-10-2	The approved cybersecurity awareness program shall be implemented within the entity.
1-10-3	The cybersecurity awareness program shall include how to protect the entity against the most important and latest cyber risks and threats, including: 1.10.3.1 Secure handling of email services, especially phishing emails. 1.10.3.2 Secure handling of mobile devices and storage media. 1.10.3.3 Secure Internet browsing. 1.10.3.4 Secure usage of social media.
1-10-4	Specialized skills and necessary training shall be provided to personnel in positions that are linked directly to cybersecurity within the entity. Such skills and training shall be classified in line with their cybersecurity responsibilities, including: 1.10.4.1 Cybersecurity department personnel. 1.10.4.2 Personnel working on software/application development and those working on information and technology assets of the entity. 1.10.4.3 Executive and supervisory positions.
1-10-5	The implementation of cybersecurity awareness program within the entity shall be periodically reviewed.



Cybersecurity Defense

2-1	Asset Management
Objective	To ensure that the entity has an accurate and updated inventory of assets, including details of all information and technology assets of the entity, in order to support the entity's operations and cybersecurity requirements to maintain the confidentiality, integrity, accuracy, and availability of information and technology assets of the entity.
Controls	
2-1-1	Cybersecurity requirements for managing information and technology assets of the entity shall be identified, documented, and approved.
2-1-2	Cybersecurity requirements for managing information and technology assets of the entity shall be implemented.
2-1-3	The policy of acceptable use of information and technology assets of the entity shall be identified, documented, approved, and communicated.
2-1-4	The policy of acceptable use of information and technology assets of the entity shall be implemented.
2-1-5	Information and technology assets of the entity shall be classified, labeled, and handled as per the relevant legislative and regulatory requirements.
2-1-6	Cybersecurity requirements for managing information and technology assets of the entity shall be periodically reviewed.
2-2	Identity and Access Management
Objective	To ensure protecting cybersecurity of logical access to information and technology assets of the entity, in order to prevent unauthorized access and restrict access to the extent necessary for accomplishment of the assigned tasks of the entity.
Controls	
2-2-1	Cybersecurity requirements for identity and access management of the entity shall be identified, documented, and approved.
2-2-2	Cybersecurity requirements for identity and access management of the entity shall be implemented.
2-2-3	Cybersecurity requirements for identity and access management of the entity shall include the following as a minimum: 2.2.3.1 Single-factor authentication based on username and password.

	2.2.3.2 Multi-factor authentication, and defining the suitable authentication factors and their numbers as well as the suitable authentication techniques based on the result of impact assessment of authentication failure and bypass for remote access and for privileged accounts. 2.2.3.3 User authorization based on identity and access control principles (Need-to-Know and Need-to-Use principle, Least Privilege principle, and Segregation of Duties principle). 2.2.3.4 Privileged access management. 2.2.3.5 Periodic review of identities and access rights.
2-2-4	The implementation of cybersecurity requirements for identity and access management of the entity shall be periodically reviewed.
2-3	Information System and Processing Facilities Protection
Objective	To ensure the protection of information systems and processing facilities, including workstations and infrastructures of the entity, against cyber risks.
Controls	
2-3-1	Cybersecurity requirements for protection of information system and processing facilities of the entity shall be identified, documented, and approved.
2-3-2	Cybersecurity requirements for protection of information systems and processing facilities of the entity shall be implemented.
2-3-3	Cybersecurity requirements for protection of information systems and processing facilities of the entity shall include the following as a minimum: 2.3.3.1 Protection from viruses, suspicious programs and activities, and malware on workstations and servers, using modern and advanced protection technologies and mechanisms, and securely managing them. 2.3.3.2 Strict restriction on the use of external storage media and their security. 2.3.3.3 Patch management for systems, applications, and devices. 2.3.3.4 Centralized clock synchronization with an accurate and trusted source, such as sources provided by the Saudi Standards, Metrology and Quality Organization (SASO).
2-3-4	The implementation of cybersecurity requirements for protection of the information system and processing facilities of the entity shall be periodically reviewed.

2-4	Email Protection
Objective	To ensure the protection of the entity's email service against cyber risks.
Controls	
2-4-1	Cybersecurity requirements for protection of the email service of the entity shall be identified, documented, and approved.
2-4-2	Cybersecurity requirements for protection of email service of the entity shall be implemented.
2-4-3	Cybersecurity requirements for protection of the email service of the entity shall include the following as a minimum: 2.4.3.1 Analyzing and filtering email messages (specifically phishing emails and spam emails) using modern and advanced email protection techniques and mechanisms. 2.4.3.2 Multi-factor authentication, and defining the suitable authentication factors and their numbers as well as the suitable authentication techniques based on the result of impact assessment of authentication failure and bypass for remote and webmail access. 2.4.3.3 Email archiving and backup. 2.4.3.4 Secure management and protection against Advanced Persistent Threats (APT), which normally utilize zero-day malware and viruses. 2.4.3.5 Validation of the entity's email service domains by using Sender Policy Framework (SPF), Domain Keys Identified Mail (DKIM), and Domain Message Authentication Reporting and Conformance (DMARC).
2-4-4	The implementation of cybersecurity requirements for email service of the entity shall be periodically reviewed.
2-5	Networks Security Management
Objective	To ensure the protection of entity's networks against cyber risks.
Controls	
2-5-1	Cybersecurity requirements for the entity's network security management shall be identified, documented, and approved.
2-5-2	Cybersecurity requirements for the entity's network security management shall be implemented.
2-5-3	Cybersecurity requirements for the entity's network security management shall include the following as a minimum:

	2.5.3.1 Logical or physical isolation and segmentation of network segments in a secure manner which is required to control relevant cybersecurity risks, using firewall and defense-in-depth principle. 2.5.3.2 Isolation of production network from testing and development environment networks. 2.5.3.3 Secure browsing and internet connectivity, including strict restrictions on suspicious websites, file storage/sharing websites, and remote access websites. 2.5.3.4 Wireless network security and protection using secure authentication and encryption techniques and avoiding the connection of wireless networks to the entity's internal network, except after a comprehensive assessment of subsequent risks, with handling them in a way that protects the technology assets of the entity. 2.5.3.5 Restricting and managing network services, protocols, and ports. 2.5.3.6 Intrusion Prevention Systems (IPS). 2.5.3.7 Security of Domain Name Service (DNS). 2.5.3.8 Secure management and protection of Internet browsing channel against Advanced Persistent Threats (APT), which normally utilize zero-day malware and viruses. 2-5-3-9 Protecting against Distributed Denial of Service (DDoS) attacks to limit risks arising from these attacks.
2-5-4	The implementation of cybersecurity requirements for the entity's network security management shall be periodically reviewed.
2-6	Mobile Devices Security
Objective	To ensure the protection of the entity's mobile devices (including laptops, smartphones, and tablets) against cyber risks, and ensure secure handling of the entity's sensitive information and business information and protecting them during transfer and storage while using the devices of personnel of the entity (Bring Your Own Device "BYOD" policy).
Controls	
2-6-1	Cybersecurity requirements for mobile devices and BYOD security when connected to the entity's network shall be identified, documented, and approved.
2-6-2	Cybersecurity requirements for mobile devices and BYOD security of the entity shall be implemented.
2-6-3	Cybersecurity requirements for mobile devices and BYOD security of the entity shall include the following as a minimum:

	2.6.3.1 Separation and encryption of the entity's data and information stored on mobile devices and BYODs. 2.6.3.2 Controlled and restricted use based on the requirements of the interest of the entity's business. 2.6.3.3 Deletion of the entity's data and information stored on mobile devices and BYOD in cases of device loss or after the ending/termination of employment with the entity. 2.6.3.4 Security awareness for users.
2-6-4	The implementation of cybersecurity requirements for mobile devices and BYOD security of the entity shall be periodically reviewed.
2-7	Data and Information Protection
Objective	To ensure confidentiality, integrity, accuracy, and availability of the entity's data and information, as per the entity's regulatory policies and procedures and the relevant legislative and regulatory requirements
Controls	
2-7-1	Cybersecurity requirements for protecting and handling data and information of the entity shall be identified, documented, and approved, as per the relevant legislative and regulatory requirements.
2-7-2	Cybersecurity requirements for protecting data and information of the entity shall be implemented, based on its classification level.
2-7-3	The implementation of cybersecurity requirements for protecting data and information of the entity shall be periodically reviewed.
2-8	Cryptography
Objective	To ensure the proper and efficient use of cryptography to protect electronic information assets of the entity, as per the entity's regulatory policies and procedures and the relevant legislative and regulatory requirements.
Controls	
2-8-1	Cybersecurity requirements for cryptography within the entity shall be identified, documented, and approved.
2-8-2	Cybersecurity requirements for cryptography within the entity shall be implemented.
2-8-3	Cybersecurity requirements for cryptography shall include at least the requirements in the National Cryptographic Standards, published by NCA. The appropriate cryptographic standard level shall be implemented based on the nature and sensitivity of the data, systems, and networks to be protected as well as the entity's risk assessment,

	and as per the relevant legislative and regulatory requirements, as follows: 2.8.3.1 Approved cryptographic systems and solutions standards and their technical and regulatory restrictions. 2.8.3.2 Secure management of cryptographic keys during their lifecycles. 2.8.3.3 Encryption of data in-transit and at-rest, as per their classification and the relevant legislative and regulatory requirements.
2-8-4	The implementation of cybersecurity requirements for cryptography within the entity shall be periodically reviewed.
2-9	Backup and Recovery Management
Objective	To ensure the protection of the entity's data, information, and technical configurations of systems and applications against cyber risks, as per the entity's regulatory policies and procedures and the relevant legislative and regulatory requirements.
Controls	
2-9-1	Cybersecurity requirements for backup and recovery management within the entity shall be identified, documented, and approved.
2-9-2	Cybersecurity requirements for backup and recovery management within the entity shall be implemented.
2-9-3	Cybersecurity requirements for backup and recovery management shall include the following as a minimum: 2.9.3.1 Scope of backups to cover critical technology and information assets. 2.9.3.2 Ability to perform quick recovery of data and systems after cybersecurity incidents. 2.9.3.3 Periodic testing for the effectiveness of backup recovery.
2-9-4	The implementation of cybersecurity requirements for backup and recovery management within the entity shall be periodically reviewed.
2-10	Vulnerabilities Management
Objective	To ensure timely detection and effective remediation of technical vulnerabilities to prevent or minimize the probability of exploitation of these vulnerabilities by cyber-attacks and to reduce any impacts on the entity's business.
Controls	
2-10-1	Cybersecurity requirements for technical vulnerabilities management within the entity shall be identified, documented, and approved.
2-10-2	Cybersecurity requirements for technical vulnerabilities management within the entity shall be implemented.

2-10-3	Cybersecurity requirements for technical vulnerabilities management shall include the following as a minimum: 2.10.3.1 Periodic vulnerabilities assessment and detection. 2.10.3.2 Vulnerabilities classification based on their severities. 2.10.3.3 Vulnerabilities remediation based on their classification and the associated cyber risks. 2.10.3.4 Patch management to remediate vulnerabilities, and ensuring the integrity and effectiveness of these updates and fixes are verified using a non-production environment before being applied. 2.10.3.5 Communication and subscription with trusted resources for new and up-to-date vulnerabilities.
2-10-4	The implementation of cybersecurity requirements for technical vulnerabilities management within the entity shall be periodically reviewed.
2-11	Penetration Testing
Objective	To assess and test the efficiency of the entity's cybersecurity defense capabilities through simulation of actual cyber-attack methods and technologies to discover unknown weaknesses that may lead to cyber penetration of the entity, as per the relevant legislative and regulatory requirements.
Controls	
2-11-1	Cybersecurity requirements for penetration testing within the entity shall be identified, documented, and approved.
2-11-2	Cybersecurity requirements for penetration testing within the entity shall be implemented.
2-11-3	Cybersecurity requirements for penetration testing shall include the following as a minimum: 2.11.3.1 Scope of penetration testing to include all externally provided services (via the Internet) and their technical components, including infrastructure, websites, web applications, smartphone and tablet applications, email, and remote access. 2.11.3.2 Conducting penetration tests periodically.
2-11-4	The implementation of cybersecurity requirements for penetration testing shall be periodically reviewed.

2-12	Cybersecurity Event Logs and Monitoring Management
Objective	To ensure timely collection, analysis, and monitoring of cybersecurity event logs for proactive detection and effective management of cyber-attacks to prevent or minimize negative impacts on the entity's business.
Controls	
2-12-1	Cybersecurity requirements for cybersecurity event logs and monitoring management within the entity shall be identified, documented, and approved.
2-12-2	Cybersecurity requirements for cybersecurity event logs and monitoring management within the entity shall be implemented.
2-12-3	Cybersecurity requirements for cybersecurity event logs and monitoring management shall include the following as a minimum: 2.12.3.1 Activation of cybersecurity event logs for critical information assets within the entity. 2.12.3.2 Activation of cybersecurity event logs for critical and privileged accounts accessing information assets as well as for remote access events within the entity. 2.12.3.3 Identification of Security Information and Event Management (SIEM) techniques required for cybersecurity event logs collection. 2.12.3.4 Continuous monitoring of cybersecurity event logs. 2.12.3.5 Retention period of cybersecurity event logs (shall be at least 12 months).
2-12-4	The implementation of cybersecurity requirements for cybersecurity event logs and monitoring management within the entity shall be periodically reviewed.
2-13	Cybersecurity Incident and Threat Management
Objective	To ensure timely identification, detection, and effective management of cybersecurity incidents and proactive response to cybersecurity threats to prevent or minimize impacts on the entity's business, as per High Order No. 37140, dated 14/08/1438H.
Controls	
2-13-1	Requirements for cybersecurity incident and threat management within the entity shall be identified, documented, and approved.
2-13-2	Requirements for cybersecurity incident and threat management within the entity shall be implemented.

2-13-3	Requirements for cybersecurity incident and threat management shall include the following as a minimum: 2.13.3.1 Cybersecurity incident response plans and escalation procedures. 2.13.3.2 Cybersecurity incident classification. 2.13.3.3 Reporting cybersecurity incidents to the NCA. 2.13.3.4 Sharing cybersecurity incident notifications, threat intelligence, penetration indicators, and incident reports with the NCA. 2.13.3.5 Collecting and handling threat intelligence feeds.
2-13-4	The implementation of cybersecurity requirements for incident and threat management within the entity shall be periodically reviewed.
2-14	Physical Security
Objective	To ensure the protection of information and technology assets of the entity against unauthorized physical access, loss, theft, and damage.
Controls	
2-14-1	Cybersecurity requirements for protection of information and technology assets of the entity against unauthorized physical access, loss, theft, and damage shall be identified, documented, and approved.
2-14-2	Cybersecurity requirements for protection of information and technology assets of the entity against unauthorized physical access, loss, theft, and damage shall be implemented.
2-14-3	Cybersecurity requirements for protection of information and technology assets of the entity against unauthorized physical access, loss, theft, and damage shall include the following as a minimum: 2.14.3.1 Authorized access to critical areas within the entity (e.g. the entity's data center, disaster recovery center, critical information processing facilities, security surveillance center, network connection rooms, technical device and equipment supply areas, etc.). 2.14.3.2 Access and monitoring logs (CCTV). 2.14.3.3 Protection of access and monitoring log information. 2.14.3.4 Security of the destruction and re-use of physical assets that hold classified information (including paper documents and storage media). 2.14.3.5 Security of devices and equipment inside and outside the entity's facilities.
2-14-4	Cybersecurity requirements for protection of information and technology assets of the entity against unauthorized physical access, loss, theft, and damage shall be periodically reviewed.

2-15	Web Application Security
Objective	To ensure the protection of external web applications of the entity against cyber risks.
Controls	
2-15-1	Cybersecurity requirements for protection of external web applications of the entity shall be identified, documented, and approved.
2-15-2	Cybersecurity requirements for protection of external web applications of the entity shall be implemented.
2-15-3	Cybersecurity requirements for protection of external web applications of the entity shall include the following as a minimum: 2.15.3.1 Use of web application firewall. 2.15.3.2 Adoption of the multi-tier architecture principle. 2.15.3.3 Use of secure protocols (e.g. HTTPS). 2.15.3.4 Clarification of the secure usage policy for users. 2.15.3.5 User authentication, and the suitable authentication factors and their numbers as well as the authentication techniques shall be defined based on the result of impact assessment of authentication failure and bypass for users' access.
2-15-4	Cybersecurity requirements for protection of web applications of the entity shall be periodically reviewed.



Cybersecurity Resilience

3-1	Cybersecurity Resilience Aspects of Business Continuity Management (BCM)
Objective	To ensure the inclusion of cybersecurity resilience requirements in the entity's business continuity management and remediate and minimize the impacts of disruptions on the entity's critical e-services and information processing systems and facilities caused by cyber risks.
Controls	
3-1-1	Cybersecurity requirements for business continuity management within the entity shall be identified, documented, and approved.
3-1-2	Cybersecurity requirements for business continuity management within the entity shall be implemented.
3-1-3	Cybersecurity requirements for business continuity management within the entity shall include the following as a minimum: 3.1.3.1 Ensuring the continuity of cybersecurity systems and procedures. 3.1.3.2 Developing plans for response to cybersecurity incidents that may affect the entity's business continuity. 3.1.3.3 Developing disaster recovery plans.
3-1-4	Cybersecurity requirements for business continuity management within the entity shall be periodically reviewed.



Third-Party and Cloud Computing Cybersecurity

4-1	Third-Party Cybersecurity
Objective	To ensure the protection of the entity's assets against third-party cybersecurity risks (including Information Technology (IT) outsourcing, cybersecurity outsourcing, and managed services), as per the entity's regulatory policies and procedures and the relevant legislative and regulatory requirements.
Controls	
4-1-1	Cybersecurity requirements for the entity's contracts and agreements with third parties shall be identified, documented, and approved.
4-1-2	Cybersecurity requirements for contracts and agreements with third parties, e.g. Service Level Agreement (SLA), which, if impaired, may affect the entity's data or services shall include the following as a minimum: 4.1.2.1 Clauses of non-disclosure and the secure removal of the entity's data by the third party upon the end of service. 4.1.2.2 Communication procedures in case of the occurrence of a cybersecurity incident. 4.1.2.3 Obligating the third party to apply the entity's cybersecurity requirements and policies and the relevant legislative and regulatory requirements.
4-1-3	Cybersecurity requirements for contracts and agreements with third parties providing IT or cybersecurity outsourcing or managed services shall include the following as a minimum: 4.1.3.1 Conducting a cybersecurity risk assessment and ensuring the availability of risk mitigation controls before signing contracts and agreements or upon making changes to the relevant legislative and regulatory requirements. 4.1.3.2 Cybersecurity managed service centers for monitoring and operations which use remote access shall be fully located in the Kingdom of Saudi Arabia.
4-1-4	Cybersecurity requirements for third parties shall be periodically reviewed.

4-2	Cloud Computing and Hosting Cybersecurity
Objective	To ensure proper and efficient remediation of cyber risks and implementation of cybersecurity requirements for cloud computing and hosting, as per the entity's regulatory policies and procedures, relevant legislative and regulatory requirements, orders, and decisions, and to ensure the protection of the entity's information and technology assets on cloud computing services hosted, processed, or managed by third parties.
Controls	
4-2-1	Cybersecurity requirements for use of cloud computing and hosting services shall be identified, documented, and approved.
4-2-2	Cybersecurity requirements for the cloud computing and hosting services within the entity shall be implemented.
4-2-3	In accordance with the relevant legislative and regulatory requirements, and in addition to the applicable controls in the Main Domains (1), (2), and (3) and Subdomain (4.1) that are necessary to protect the entity's data or services provided thereto, cybersecurity requirements for use of cloud computing and hosting services shall include the following as a minimum: 4.2.3.1 Protection of entity's data by cloud and hosting service providers in accordance with its classification level and returning data (in a usable format) upon service completion. 4.2.3.2 Separation of the entity's environment (especially virtual servers) from environments of other entities within the cloud computing service provider.
4-2-4	Cybersecurity requirements for cloud computing and hosting services shall be periodically reviewed.

Appendices

Appendix (A): Terms and Definitions

Table (2) below highlights some of the terms and their definitions which were used in this document.

TABLE 2 TERMS AND DEFINITION

Term	Definition
Advanced Persistent Threats (APT) Protection	Protection against advanced threats that use invisible techniques to gain unauthorized access to technology systems and networks and stay as long as possible by circumventing detection and protection tools. To accomplish this, zero-day malware are usually used in these techniques.
Asset	Any tangible or intangible thing of value to the entity. There are many types of assets, and some of which are obvious, such as persons, machinery, facilities, patents, software, and services. The term could also include less obvious things, such as information and characteristics (such as the entity's reputation and public image, as well as skills and knowledge).
Attack	Any kind of malicious activity aimed at gaining unauthorized access to, collecting, disabling, preventing, destroying, or sabotaging information system resources or the information itself.
Audit	Independent review and examination of records and activities, in order to assess the effectiveness of cybersecurity controls and to ensure compliance with policies, operational procedures, standards, and relevant legislative and regulatory requirements.
Authentication	Verification of the user's identity, process, or device, which is often a prerequisite for allowing access to resources on the system.
Authorization	The property of identifying and verifying the rights/licenses of the user to access the information and technology assets and resources of the entity and allowing access based on the user's rights/licenses previously defined.
Availability	Ensuring timely access and use of information, data, systems, and applications.

Backup	Files, devices, data, and procedures available for use in case of failure or loss, or in case of deletion or suspension of their original copies.
Bring Your Own Device (BYOD)	This term refers to an entity's policy that allows (in whole or in part) its personnel to bring their personal devices (laptops, tablets, and smartphones) to their workplace within the entity and use such devices to access the entity's networks, information, applications, and systems to which access is restricted.
Change Management	A service management system that ensures a systematic and proactive approach using effective standard methods and procedures (for example, change in the entity's infrastructure and networks, etc.). Change management helps all stakeholders, including individuals and teams alike, move from their current state to the next desired state. It also helps reduce the impact of relevant incidents on service.
Closed-Circuit Television (CCTV)	CCTV, also known as video surveillance, uses video cameras to transmit a signal to a specific location on a limited set of screens. This term is often used to refer to the surveillance technique employed in areas that require monitoring due to the importance of physical security.
Cloud Computing	A model to enable on-demand access to a shared pool of information technology resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provided and launched with minimal operational management effort and service setup intervention/interaction from the service provider. Cloud computing allows users to access technology-based services over a cloud computing network without needing to know or control the technology infrastructure that supports them. Cloud computing models are composed of five essential characteristics: on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service. There are three models of cloud computing services: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). Moreover, according to the nature of access, there are four cloud computing models: Public Cloud Computing, Community Cloud Computing, Private Cloud Computing, and Hybrid Cloud Computing.
Compromise	Disclosure or acquisition of information not authorized to be leaked to or obtained by third parties, or violation of the entity's cybersecurity

	policy through the disclosure, alteration, sabotage, or loss of anything, either intentionally or unintentionally. Compromise also means the disclosure, acquisition, leakage, alteration, or use of sensitive data without authorization (including cryptographic keys and other critical cybersecurity standards).
Sensitive Data/Information	Information (or data) that is highly sensitive and important, as classified by the entity, and intended for their use. One of the methods that can be used to classify this type of information is to measure the extent of damage when it is disclosed, accessed in an unauthorized manner, lost, or sabotaged, as this may result in material or moral damage to the entity or its clients, affecting the lives of persons associated with that information, or affecting and damaging the State security, national economy, or national capacities. Sensitive information includes all information whose unauthorized disclosure, loss, or sabotage results in accountability or statutory penalties.
Confidentiality	Maintaining authorized restrictions on access to and disclosure of information, including means of privacy/personal information protection.
Critical National Infrastructure (CNI)	Essential elements of infrastructure (i.e. assets, facilities, systems, networks, processes, and key personnel who operate and process them) whose loss or compromise may result in: ● Significant negative impact on the availability, integration, or delivery of basic services, including services whose integrity could, if compromised, result in serious loss of property, lives, and/or injuries, taking into account significant national-level economic and/or social impacts. ● Significant impact on national security, national defense, and/or State economy or national capacities.
Cryptography	It is also called (cryptology). It refers to rules that include the principles, methods, and means of storing and transmitting data or information in a particular form, in order to conceal its semantic content and prevent unauthorized use or prevent undetected modification, so that only the concerned persons can read and process them.
Cyber-Attack	An intentional attempt to impact cybersecurity negatively, whether successful or not.
Cyber Risks	Risks that harm the entity's business operations (including the entity's vision, mission, management, image, or reputation), assets, individuals,

	other entities, or the State due to unauthorized access, use, disclosure, disruption, modification, or damage of information and/or information systems.
Cybersecurity	Pursuant to the provisions of the NCA's Statute issued by Royal Order No. 6801, dated 11/02/1439H., cybersecurity is the protection of networks, IT systems, operational technologies systems, their hardware and software components, services, and the data they contain, from any unauthorized penetration, disruption, modification, access, use, or exploitation. The concept of cybersecurity also encompasses information security, digital security, and the like.
Cybersecurity Resilience	The overall ability of entities to withstand cyber events and, where harm is caused, recover from them.
Cyberspace	The interconnected network of IT infrastructure, including the Internet, communication networks, computer systems, Internet-connected devices, and associated processors and control devices. The term can also refer to a virtual world or domain, such as experimental phenomenon or abstract concept.
Data and Information Classification	Determining the sensitivity level of data and information which gives rise to security controls for each classification level. Data and information sensitivity levels are set according to predefined categories, where data and information is created, modified, improved, stored, or transmitted. The classification level is an indicator of the value or significance of data and information to the entity.
Data Archiving	The process of transferring data that is no longer actively used to a separate storage device for long-term retention. Archive data consists of older data that is still important to the entity and may be needed for future reference, as well as data that shall be retained for legal and regulatory compliance purposes.
Defense-in-Depth	A concept of information assurance where multiple levels of security controls are used (as a defense) in the IT/OT system.
Disaster Recovery	Programs, activities, and plans designed to restore the entity's critical business functions and services to an acceptable state, following exposure to cyber-attacks or disruption of such functions or services.
Domain Name System (DNS)	A technical system that uses a database distributed over the network and/or the Internet to allow the translation of domain names into IP addresses and vice versa, in order to identify service addresses, such as web and e-mail servers.

Effectiveness	A degree whereby a planned impact is achieved. Planned activities are considered effective if they are already implemented, and planned results are considered effective if they are already achieved. The Key Performance Indicators (KPIs) can be used to measure and evaluate the effectiveness level.
Efficiency	Relationship between the results achieved (outputs) and the resources used (inputs). The efficiency of a process or system can be enhanced by achieving more results using the same resources (inputs) or even less.
Event	An event related to the cybersecurity state of a network, a system, a service, data, or any other digital device.
Hyper Text Transfer Protocol Secure (HTTPS)	A protocol that uses encryption to secure the web pages and data when they are transmitted over the network. It is a secure version of the Hyper Text Transfer Protocol (HTTP).
Identification	A means for verifying the user's identity, process, or device, which is usually a prerequisite for granting access to system resources.
Incident	An event that occurred and negatively impacted cybersecurity, whether intentional or unintentional.
Integrity	Protection against unauthorized modification or destruction of information, including ensuring information non-repudiation and reliability.
International Requirements	International requirements are those developed by an international entity or organization for regulatory use worldwide (e.g. SWIFT, PCI, etc.).
Intrusion Prevention System (IPS)	A system with intrusion detection capabilities, as well as capabilities to prevent and stop suspicious or potential activities and incidents.
Key Performance Indicator (KPI)	A type of performance measurement tools that evaluate the success of an activity or an entity in achieving specific objectives.
Labeling	Display of information (with specific and standard naming and coding) on the entity's assets (such as devices, applications, documents, etc.) to refer to some information on the classification, ownership, and type of the asset and other asset management information.
Least Privilege	A basic principle in cybersecurity that aims at granting users only access privileges they need to fulfill their official responsibilities.
Malware	A program that infects systems, usually covertly, with the intent of compromising the confidentiality, integrity, accuracy, or availability of data, applications, or operating system.

Multi-Factor Authentication (MFA)	A security system that verifies user identity, using several authentication factors through authentication technique. Authentication factors are: ● Knowledge (something only the user knows “like using password technique”). ● Possession (something only owned by the user “such as using technique like a program, device generating random numbers or SMSs” for login records, which are called: One-Time-Password). ● Inherent characteristics (characteristics of the user only, such as using fingerprint or face recognition techniques).
Multi-tier Architecture	An architecture or structure that applies a client-server approach in which the functional process logic, data access, data storage, and user interface are developed and maintained as separate units on separate platforms.
Need-to-Know and Need-to-Use	Restrictions on data, which is considered confidential, unless a person has a specific need to know for official business duties.
Offline/Offsite Backup	A backup of databases, and settings of systems, applications, and devices when the copy is offline and cannot be updated. Typically, backup tapes are utilized for offsite backup.
Online Backup	A storage method whereby the backup is regularly taken on a remote server over a network (either within the entity’s network or hosted by a service provider).
Organization Staff	Individuals who work for the entity (including official employees, temporary employees, and contractors).
Outsourcing	Obtaining goods or services by contracting with a supplier or a service provider.
Patch	Supporting data packages used to upgrade, fix, or improve computer operating system, software, or applications. This includes fixing security vulnerabilities and other bugs. Such patches are usually called fixes, bug fixes, and usability or performance improvements.
Penetration Testing	Testing a computer system, network, web application, or mobile application to find vulnerabilities that can be exploited by an attacker.

Phishing Emails	An attempt to obtain confidential information, such as usernames, passwords, or credit card details, often for malicious reasons and intentions, by disguising as a trustworthy entity in emails.
Physical Security	Physical security describes security measures designed to prevent unauthorized access to the entity's facilities, equipment, and resources, and to protect individuals and property against damage or harm (such as espionage, theft, or terrorist attacks). Physical security involves the use of multiple tiers of interconnected systems, including CCTV, security guards, security limits, locks, access control systems, and many other technologies.
Policy	A document with clauses specifying a general obligation, direction, or intent as formally expressed by the Authorized Official of the entity. Cybersecurity policy is a document with clauses reflecting official commitment of the senior management of the entity to implement and improve the cybersecurity program within the entity. Such policy includes the entity's objectives relating to the cybersecurity program, as well as its controls, requirements, and improvement and development mechanisms.
Privileged Access Management	The process of managing high-risk authorizations on the entity's systems, which often need special handling to minimize risks that may arise from the misuse thereof.
Procedure	A document with a detailed description of the steps necessary to perform specific operations or activities in compliance with relevant standards and policies. Procedures are defined as part of operations.
Process	A set of interrelated or interactive activities that translates inputs into outputs. Such activities are influenced by the entity's policies.
Recovery	A procedure or process to restore or control something that is suspended, damaged, stolen, or lost.
Retention	The time period during which information, data, event logs, or backups shall be retained, regardless of the form (e.g. paper, electronic, etc.).
Secure Coding Standards	A practice for the development of computer software and applications in a way that protects against exposure to cybersecurity vulnerabilities in software and applications.

Secure Configuration and Hardening	Protecting, hardening, and configuring the settings of computers, systems, applications, network devices, and security devices to resist cyber-attacks, such as disabling or changing manufacturing and default accounts, disabling unused services, and disabling unused network ports.
Security Information and Event Management (SIEM)	A system that manages and analyzes security event logs in real time, in order to monitor threats and analyze the results of interrelated rules for event logs and reports on logs data, and incident response.
Security Testing	A process intended to ensure that a modified or new system or application, has the appropriate security controls and protection, is free from any security vulnerabilities that might compromise other systems and applications or lead to misusing the system or application or information thereon, and to maintain the functionality of the system or application as intended.
Security-by-Design	A methodology for developing systems and software and designing networks to free them from cybersecurity vulnerabilities and weaknesses and make them impervious to cyber-attack as much as possible through several measures, such as continuous testing, authentication safeguards, and adherence to best programming and design practices.
Segregation of Duties	A key cybersecurity principle that aims at minimizing errors and fraud during the stages of processing specific tasks, by ensuring the presence of more than one individual to complete a task with different privileges.
Sender Policy Framework	A method to verify that the email server used for sending emails belongs to the sender's domain.
Third-Party	Any entity that serves as a party to contractual relationship to provide goods or services (including suppliers and service providers).
Threat	Anything with the potential to impact cybersecurity negatively.
Threat Intelligence	It provides and analyzes organized information on recent, current, and potential attacks that could pose a cyber threat to the entity.
Vulnerability	A weakness in any information technology asset (such as software and systems) or a process, control, or anything, that could be exploited to negatively impact cybersecurity.

Web Application Firewall	A protection system that is installed before web applications to minimize risks that may arise from attack attempts against web applications.
Zero-Day Malware	Previously unknown malware that has been produced or disseminated recently and is normally hard to be detected by prior knowledge of malware (Signature-based Protection).

Appendix (B): List of the Abbreviations

Table (3) below shows some of the abbreviations and their meanings which are used in this document.

TABLE 3 LIST OF ABBREVIATIONS

Abbreviation	Full Term
APT	Advanced Persistent Threat
BCM	Business Continuity Management
BYOD	Bring Your Own Device
CCTV	Closed-Circuit Television
CNI	Critical National Infrastructure
DDoS	Distributed Denial of Service Attack
DKIM	Domain Keys Identified Mail
DMARC	Domain Message Authentication Reporting and Conformance
DNS	Domain Name System
ECC	Essential Cybersecurity Controls
HTTPS	Hyper Text Transfer Protocol Secure
ICT	Information and Communication Technology
IT	Information Technology
MFA	Multi-Factor Authentication
OT	Operational Technology
SIEM	Security Information and Event Management
SLA	Service Level Agreement
SPF	Sender Policy Framework

Appendix (C): List of Updates

Table (4) below illustrates the updates on the previous version (i.e., ECC-1:2018).

TABLE 4 LIST OF UPDATES

Version		Date		
ECC – 2 : 2024		2024		
Update type	Section	Previous text	Updated text	Rationale
Modification	ECC Scope of Work	These controls are applicable to government entities in the Kingdom of Saudi Arabia (including ministries, authorities, establishments and others) and its companies and entities.	These Controls are applicable to government agencies in the Kingdom of Saudi Arabia (including ministries, authorities, establishments and others) and their affiliated companies and entities (inside and outside the kingdom)	Clarification
Deletion	ECC Statement of Applicability	Controls in main domain 5 (Industrial Control Systems Cybersecurity) are applicable and must be implemented by entities currently using or planning to use industrial control systems.		Deletion of main domain 5. Controls in domain 5 moved to the OTCC (Operational Technology Cybersecurity Controls)
Modification	Control 1-2-2	The position of cybersecurity function head (e.g., CISO), and related supervisory and critical positions within the function, must be filled with full-time and experienced	All cybersecurity positions shall be filled out with full-time and qualified Saudi cybersecurity professionals.	Cybersecurity enhancement

Version		Date		
ECC – 2 : 2024		2024		
Update type	Section	Previous text	Updated text	Rationale
		Saudi cybersecurity professionals.		
Deletion	Control 1-7-1	The entity must comply with related national cybersecurity laws and regulations.		Cybersecurity regulatory maturity, and supporting entities' compliance
Modification	Control 1-7-2	The entity must comply with any nationally-approved international agreements and commitments related to cybersecurity.	If there are nationally approved international agreements or commitments that include cybersecurity requirements, the entity shall identify and comply with these requirements.	Clarification
Modification	Sub-control 2-2-3-1	User authentication based on username and password.	Single-factor authentication based on username and password.	Clarification
Modification	Sub-control 2-2-3-2	Multi-factor authentication for remote access.	Multi-factor authentication, and defining the suitable authentication factors and their numbers as well as the suitable authentication techniques based on the result of impact assessment of authentication failure and bypass for remote access and for privileged accounts.	Clarification

Version		Date		
ECC – 2 : 2024		2024		
Update type	Section	Previous text	Updated text	Rationale
Modification	Sub-control 2-4-3-2	Multi-factor authentication for remote and webmail access to email service.	Multi-factor authentication, and defining the suitable authentication factors and their numbers as well as the suitable authentication techniques based on the result of impact assessment of authentication failure and bypass for remote and webmail access.	Clarification
Modification	Sub-control 2-4-3-5	Validation of the entity's email service domains (e.g., using Sender Policy Framework (SPF)).	Validation of the entity's email service domains by using Sender Policy Framework (SPF), Domain Keys Identified Mail (DKIM), and Domain Message Authentication Reporting and Conformance (DMARC).	Clarification
Addition	Sub-control 2-5-3-9	N/A	Protecting against Distributed Denial of Service (DDoS) attacks to limit risks arising from these attacks.	Cybersecurity enhancement
Modification	Control 2-7-2	The cybersecurity requirements for protecting and handling data and information must be implemented.	Cybersecurity requirements for protecting data and information of the entity shall be implemented, based on its classification level.	Clarification
Deletion	Control 2-7-3	The cybersecurity requirements for protecting and handling data and		For the National Data Management Office (NDMO) at the Saudi

Version		Date		
ECC – 2 : 2024		2024		
Update type	Section	Previous text	Updated text	Rationale
		information must include at least the following: 2-7-3-1 Data and information ownership. 2-7-3-2 Data and information classification and labeling mechanisms. 2-7-3-3 Data and information privacy.		Data and Artificial Intelligence Authority mandates, entities must refer to the National Data Management Office regarding data privacy before taking any action in this regard.
Modification	Control 2-8-3	The cybersecurity requirements for cryptography must include at least the following: 2-8-3-1 Approved cryptographic solutions standards and its technical and regulatory limitations. 2-8-3-2 Secure management of cryptographic keys during their lifecycles. 2-8-3-3 Encryption of data in-transit and at-rest as per classification and related laws and regulations.	Cybersecurity requirements for cryptography shall include at least the requirements in the National Cryptographic Standards, published by NCA. The appropriate cryptographic standard level shall be implemented based on the nature and sensitivity of the data, systems, and networks to be protected as well as the entity's risk assessment, and as per the relevant legislative and regulatory requirements, as follows: 2.8.3.1 Approved cryptographic systems and solutions standards and their technical and regulatory restrictions.	Clarification

Version		Date		
ECC – 2 : 2024		2024		
Update type	Section	Previous text	Updated text	Rationale
			2.8.3.2 Secure management of cryptographic keys during their lifecycles. 2.8.3.3 Encryption of data in-transit and at-rest, as per their classification and the relevant legislative and regulatory requirements.	
Modification	Sub-control 2-15-3-5	Multi-factor authentication for users' access.	User authentication, and the suitable authentication factors and their numbers as well as the authentication techniques shall be defined based on the result of impact assessment of authentication failure and bypass for users' access.	Clarification
Modification	Objective of Sub-domain 4-1	To ensure the protection of assets against the cybersecurity risks related to third-parties including outsourcing and managed services as per organizational policies and procedures, and related laws and regulations.	To ensure the protection of the entity's assets against third-party cybersecurity risks (including Information Technology (IT) outsourcing, cybersecurity outsourcing, and managed services), as per the entity's regulatory policies and procedures and the relevant legislative and regulatory requirements.	Clarification
Modification	Control 4-1-3	The cybersecurity requirements for contracts and agreements with IT	Cybersecurity requirements for contracts and agreements with third	Clarification

Version		Date		
ECC – 2 : 2024		2024		
Update type	Section	Previous text	Updated text	Rationale
		outsourcing and managed services third-parties must include at least the following:	parties providing IT or cybersecurity outsourcing or managed services shall include the following as a minimum:	
Modification	Control 4-2-3-1	Classification of data prior to hosting on cloud or hosting services and returning data (in a usable format) upon service completion.	Protection of entity's data by cloud and hosting service providers in accordance with its classification level and returning data (in a usable format) upon service completion.	Cybersecurity enhancement
Deletion	Sub-control 4-2-3-3	Entity's information hosting and storage must be inside the Kingdom of Saudi Arabia.		Controls related to data localization have been transferred from the document to the National Data Management Office (NDMO) at the Saudi Data and Artificial Intelligence Authority for as per the mandates, and entities must refer to the National Data Management Office regarding data localization before taking any action in this regard.
Deletion	Main domain 5	Industrial Control Systems Cybersecurity		Controls in domain 5 moved to the OTCC

Version		Date		
ECC – 2 : 2024		2024		
Update type	Section	Previous text	Updated text	Rationale
				(Operational Technology Cybersecurity Controls)
Modification	Terms and Definitions	Confidential Data/Information	Sensitive Data/Information	Translation update
Modification	Terms and Definitions	Critical National Infrastructure (CNI) These are the assets (i.e., facilities, systems, networks, processes and key operators who operate and process them), whose loss or vulnerability to security breaches may result in: ● Significant negative impact on the availability, integration or delivery of basic services, including services that could result in serious loss of property and/or lives and/or injuries, alongside observance of significant economic and/or social impacts. ● Significant impact on national security and/or national defense and/or state economy or national capacities.	Critical National Infrastructure (CNI) Essential elements of infrastructure (i.e. assets, facilities, systems, networks, processes, and key personnel who operate and process them) whose loss or compromise may result in: ● Significant negative impact on the availability, integration, or delivery of basic services, including services whose integrity could, if compromised, result in serious loss of property, lives, and/or injuries, taking into account significant national-level economic and/or social impacts. ● Significant impact on national security, national defense, and/or	Clarification

Version		Date		
ECC – 2 : 2024		2024		
Update type	Section	Previous text	Updated text	Rationale
			State economy or national capacities.	
Modification	Terms and Definitions	Cyber Attack Intentional exploitation of computer systems, networks, and entities whose work depends on digital ICT, in order to cause damage.	Cyber Attack An intentional attempt to impact cybersecurity negatively; whether succeeded or not.	Clarification
Modification	Terms and Definitions	Event Something that happens in a specific place (such as network, system, application) at a specific time.	Event An event related to the cybersecurity state of a network, or a system, or a service, or data, or any other digital device.	Clarification
Modification	Terms and Definitions	Incident A compromise through violation of cybersecurity policies, acceptable use policies, practices or cybersecurity controls or requirements.	Incident An event that occurred and negatively impacted cybersecurity, whether intentional or unintentional.	Clarification
Modification	Terms and Definitions	(Inter)National Requirements National requirements are those developed by a regulatory entity or body in Saudi Arabia for regulatory use (e.g., NCA's Essential Cybersecurity Controls (ECC-1:2018))	International Requirements International requirements are those developed by an international entity or organization for regulatory use worldwide (e.g. SWIFT, PCI, etc.).	Clarification

Version		Date		
ECC – 2 : 2024		2024		
Update type	Section	Previous text	Updated text	Rationale
		International requirements are those developed by a global entity for worldwide regulatory or best practices use (e.g., SWIFT, PCI-DSS, etc.).		
Modification	Terms and Definitions	Multi-Factor Authentication (MFA) A security system that verifies user identity, which requires the use of several separate elements of identity verification mechanisms. Verification mechanisms include several elements: ● Knowledge (something only the user knows “like password”). ● Possession (something only owned by the user “such as a program, device generating random numbers or SMSs” for login records, which are called: One-Time-Password). ● Inherent characteristics (characteristics of the user only, such as fingerprint).	Multi-Factor Authentication (MFA) A security system that verifies user identity, using several authentication factors through user authentication techniques. Authentication factors are: ● Knowledge (something only the user knows “such as using a password technique”). ● Possession (something only owned by the user “such as using techniques like a program or a device generating random numbers or SMSs” for login records, which are called One-Time-Password). ● Inherent characteristics (characteristics of the user only, such as using	Clarification

Version		Date		
ECC – 2 : 2024		2024		
Update type	Section	Previous text	Updated text	Rationale
			fingerprint or face recognition techniques).	
Deletion	Terms and Definitions	Privacy Freedom from unauthorized interference or disclosure of personal information about an individual.		For the National Data Management Office (NDMO) at the Saudi Data and Artificial Intelligence Authority mandates, entities must refer to the National Data Management Office regarding data privacy before taking any action in this regard.
Modification	Terms and Definitions	Threat Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. Also, the potential for a threat-source to successfully exploit a	Threat Anything with the potential to impact cybersecurity negatively.	Clarification

Version		Date		
ECC – 2 : 2024		2024		
Update type	Section	Previous text	Updated text	Rationale
		particular information system vulnerability.		
Modification	Terms and Definitions	Vulnerability Any type of weakness in a computer system, software, application, a set of procedures, or in anything that leaves cybersecurity exposed to a threat.	Vulnerability A weakness in any information technology asset (such as software and systems) or a process, control, or anything, that could be exploited to negatively impact cybersecurity.	Clarification
Addition	List of the Abbreviations		DDoS: Distributed Denial of Service Attack DKIM: Domain Keys Identified Mail DMARC: Domain Message Authentication Reporting and Conformance SPF: Sender Policy Framework	Addition of abbreviations
Deletion	List of the Abbreviations	ICS: Industrial Control System SIS: Safety Instrumented System		Controls in domain 5 moved to the OTCC (Operational Technology Cybersecurity Controls)



الهيئة الوطنية
للأمن السيبراني
National Cybersecurity Authority