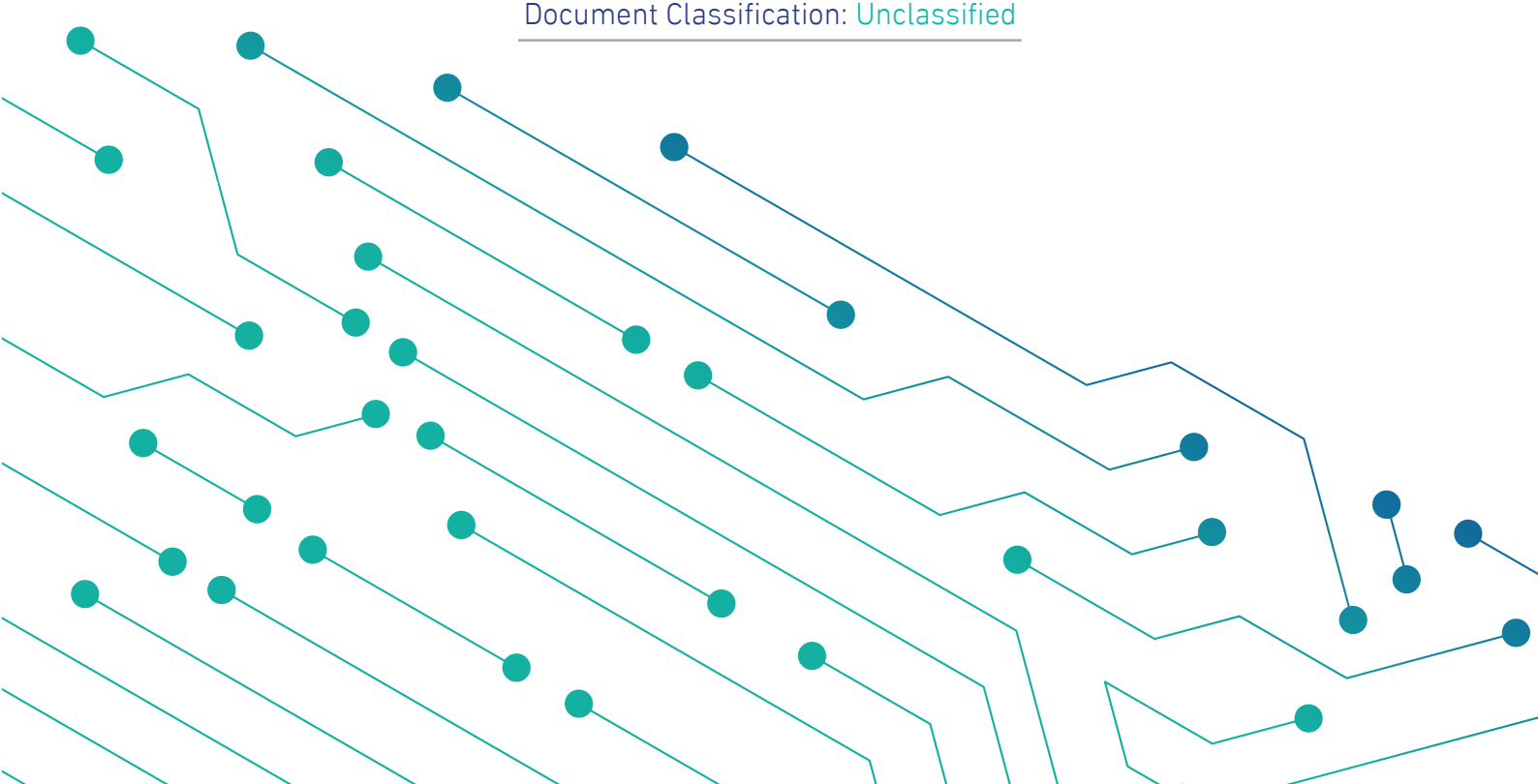


الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

Essential Cybersecurity Controls (ECC – 1 : 2018)

Sharing Indicator : White
Document Classification: Unclassified



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 interpretation of this document.

In The Name Of Allah,
The Most Benevolent,
The Most Merciful

Traffic Light Protocol (TLP):

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



Red – Personal, Confidential and for Intended 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 organization.



Amber – Restricted Sharing

The recipient may share information classified in orange only with intended recipients inside the organization and with recipients who are required to take action related to the shared information.



Green – Sharing within The Same Community

The recipient may share information classified in green with other recipients inside the organization or outside it within the same sector or related to the organization. However, it is not allowed to exchange or publish this information on public channels.



White – No Restriction

Table of Contents

Executive Summary	6
Introduction	7
Objectives	8
Scope of Work and Applicability	9
ECC Scope of Work	9
ECC Statement of Applicability	9
Implementation and Compliance	10
Evaluation and Compliance Tool	10
Update and Review	10
ECC Domains and Structure	11
Main Domains	11
Subdomains	12
Structure	13
The Essential Cybersecurity Controls (ECC)	14
1- Cybersecurity Governance	14
2- Cybersecurity Defense	19
3- Cybersecurity Resilience	26
4- Third-Party and Cloud Computing Cybersecurity	27
5- Industrial Control Systems Cybersecurity	29
Appendices	30
Appendix (A): Terms and Definitions	30
Appendix (B): List of the Abbreviations	36
List of the Tables	
Table (1): ECC Structure	13
Table (2): Terms and Definitions	30
Table (3): List of Abbreviations	36
List of the Figures & Illustrations	
Figure (1): ECC Main Domains	11
Figure (2): ECC Subdomains	12
Figure (3): Controls Coding Scheme	13
Figure (4): ECC Structure	13

Executive Summary

The Kingdom of Saudi Arabia's Vision 2030 aims at a comprehensive improvement of the nation and its security, economy and citizens' well-being. One of the essential goals of Vision 2030 is continued transformation into the digital world and improvement of the digital infrastructure in order to keep up with the accelerated global progress in digital services, renewable global networks and IT/OT systems in line with improved computer processing, massive data storage and exchange capabilities for data, in order to be prepared for handling artificial intelligence and 4th industrial revolution transformations.

This transformation requires easing the flow of information, securing it and preserving the integrity of all systems. It also requires maintaining and supporting the cybersecurity of the Kingdom in order to protect its vital interests, national security, critical infrastructures, high priority sectors and governmental services and practices. To accomplish this objective, the National Cybersecurity Authority (NCA) was established, and its mandate was approved as per the Royal Decree number 6801, dated 11/2/1439H making it the national and specialized reference for matters related to cybersecurity in the Kingdom.

NCA's mandates and duties fulfill the strategic and regulatory cybersecurity needs related to the development of cybersecurity national policies, governance mechanisms, frameworks, standards, controls and guidelines.

They also fulfill the need to continuously monitor the compliance of organizations to support the important role of cybersecurity which has increased with the rise of security risks in cyberspace more than any time before.

NCA's mandate states that its responsibility for cybersecurity does not absolve any public, private or other organization from its own cybersecurity responsibilities as confirmed by the Royal Decree number 57231, dated 10/11/1439H, which states that "all government organizations must improve their cybersecurity level to protect their networks, systems and data, and comply with NCA's policies, framework, standards, controls and guidelines"

From this perspective, NCA developed the Essential Cybersecurity Controls (ECC-1: 2018) to set the minimum cybersecurity requirements for national organizations that are within its scope of ECC implementation. This document highlights the details of these controls, goals, scope, statement of applicability, compliance approach and monitoring.

All national organizations must implement all necessary measures to ensure continuous compliance with the ECC as per item 3 of article 10 of NCA's mandate and as per the Royal Decree number 57231, dated 10/11/1439H.

Introduction

The National Cybersecurity Authority (referred to in this document as “The Authority” or “NCA”) developed the essential cybersecurity controls (ECC – 1: 2018) after conducting a comprehensive study of multiple national and international cybersecurity frameworks and standards, studying related national decisions, law and regulatory requirements, reviewing and leveraging cybersecurity best practices, analyzing previous cybersecurity incidents and attacks on government and other critical organizations, and surveying and considering opinions of multiple national organizations.

The Essential Cybersecurity Controls consist of the following:

- 5 Cybersecurity Main Domains.
- 29 Cybersecurity Subdomains.
- 114 Cybersecurity Controls.

These cybersecurity controls are linked to related national and international law and regulatory requirements.

Objectives

The main objective of these controls is to set the minimum cybersecurity requirements for information and technology assets in organizations. These requirements are based on industry leading practices which will help organizations minimize the cybersecurity risks that originate from internal and external threats. The following key objectives must be focused on in order to protect the organization's information and technology assets:

- Confidentiality
- Integrity
- Availability

These controls take into consideration the following four main cybersecurity pillars:

- Strategy
- People
- Processes
- Technology

Scope of Work and Applicability

ECC Scope of Work

These controls are applicable to government organizations in the Kingdom of Saudi Arabia (including ministries, authorities, establishments and others) and its companies and entities, as well as private sector organizations owning, operating or hosting Critical National Infrastructures (CNIs), which are all referred to herein as "The Organization". The NCA strongly encourages all other organizations 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 after taking into consideration the cybersecurity needs of all organizations and sectors in the Kingdom of Saudi Arabia. Every organization must comply with all applicable controls in this document.

Applicability to implement these cybersecurity controls depends on the organization's business and its use of certain technologies. For example:

- Controls in subdomain 4-2 (Cloud Computing and Hosting Cybersecurity) are applicable and must be implemented by organizations currently using or planning to use cloud computing and hosting services.
- Controls in main domain 5 (Industrial Control Systems Cybersecurity) are applicable and must be implemented by organizations currently using or planning to use industrial control systems.

Implementation and Compliance

To comply with item 3 of article 10 of NCA's mandate and as per the Royal Decree number 57231 dated 10/11/1439H, all organizations within the scope of these controls must implement whatever necessary to ensure continuous compliance with the controls.

NCA evaluates organizations' compliance with the ECC through multiple means such as self-assessments by the organizations, periodic reports of the compliance tool or on-site audits.

Assessment and Compliance Tool

NCA will issue a tool (ECC-1: 2018 Assessment and Compliance Tool) to organize the process of evaluation and compliance measurement against the ECC.

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.

ECC Domains and Structure

Main Domains

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

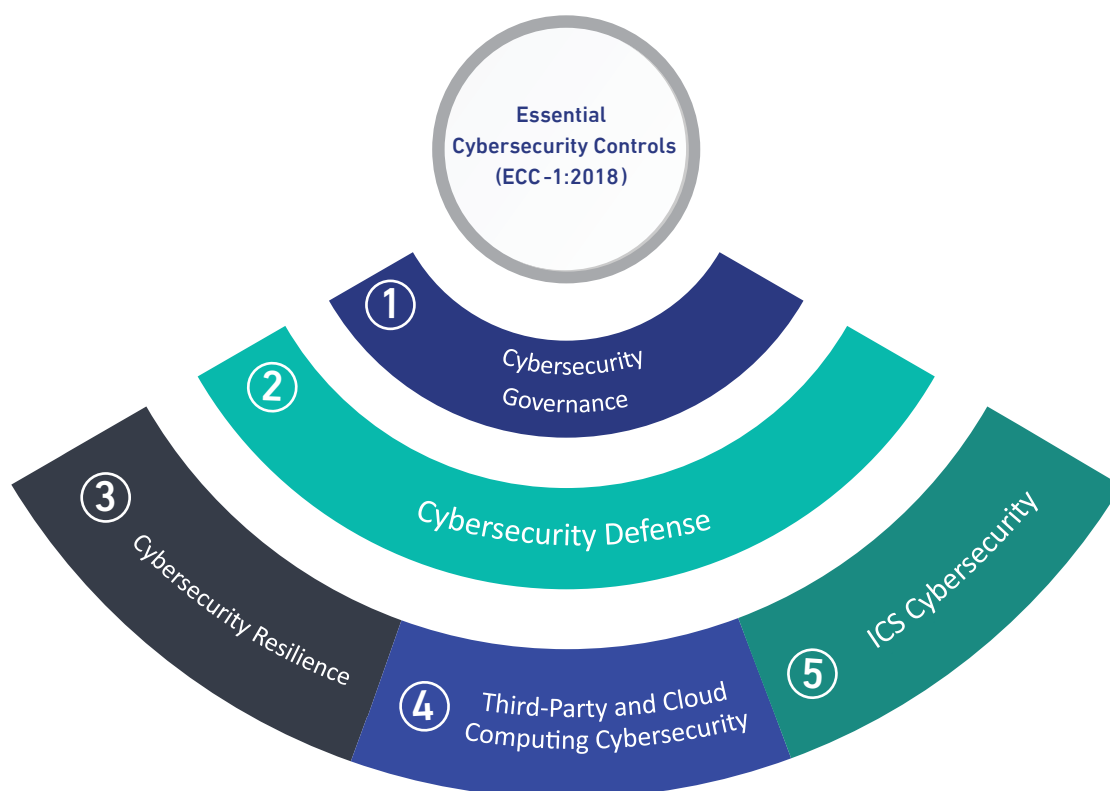


Figure (1): Main Domains of ECC

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
5. ICS Cybersecurity	5-1	Industrial Control Systems and Devices (ICS) Protection		

Figure (2): ECC Subdomains

Structure

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

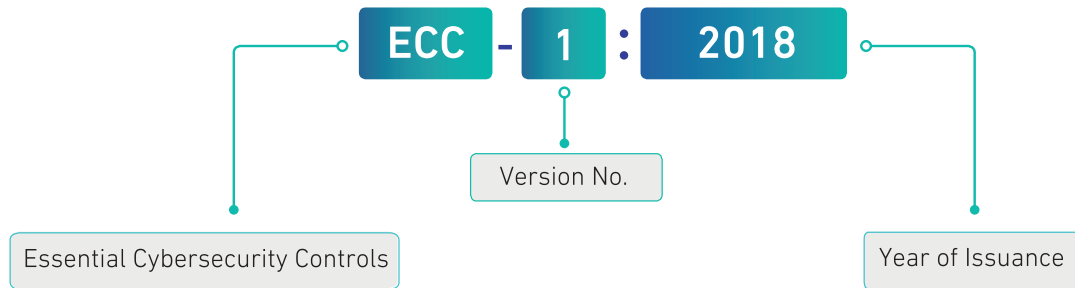


Figure (3): Controls Coding Scheme

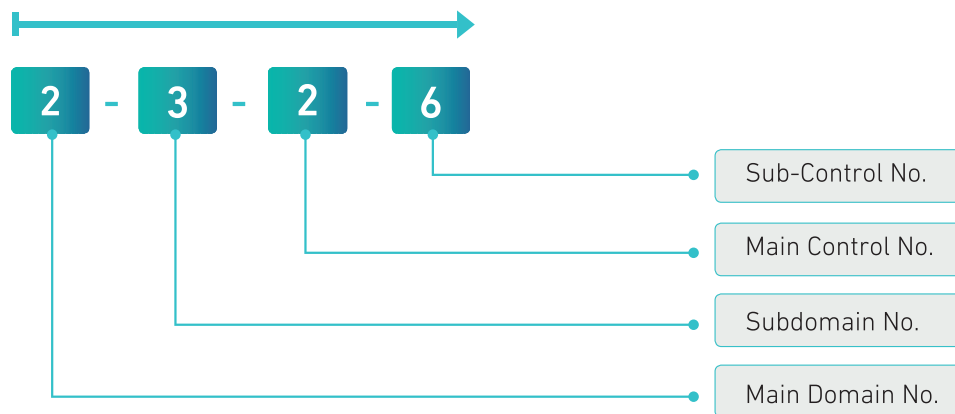


Figure (4): ECC Structure

Table (1) below shows the methodological structure of the controls.

Table (1): ECC Structure

<div>1</div> <div>Reference number of the Main Domain</div>	<div> </div> <div>Name of Main Domain</div>
Reference No. of the 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 cybersecurity plans, goals, initiatives and projects are contributing to compliance with related laws and regulations.
Controls	
1-1-1	A cybersecurity strategy must be defined, documented and approved. It must be supported by the head of the organization or his/her delegate (referred to in this document as Authorizing Official). The strategy goals must be in-line with related laws and regulations.
1-1-2	A roadmap must be executed to implement the cybersecurity strategy.
1-1-3	The cybersecurity strategy must be reviewed periodically according to planned intervals or upon changes to related laws and regulations.
1-2	Cybersecurity Management
Objective	To ensure Authorizing Official's support in implementing and managing cybersecurity programs within the organization as per related laws and regulations
Controls	
1-2-1	A dedicated cybersecurity function (e.g., division, department) must be established within the organization. This function must be independent from the Information Technology/Information Communication and Technology (IT/ICT) functions (as per the Royal Decree number 37140 dated 14/8/1438H). It is highly recommended that this cybersecurity function reports directly to the head of the organization or his/her delegate while ensuring that this does not result in a conflict of interest.
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 Saudi cybersecurity professionals.
1-2-3	A cybersecurity steering committee must be established by the Authorizing Official to ensure the support and implementation of the cybersecurity programs and initiatives within the organization. Committee members, roles and responsibilities, and governance framework must be defined, documented and approved. The committee must include the head of the cybersecurity function as one of its members. It is highly recommended that the committee reports directly to the head of the organization or his/her delegate while ensuring that this does not result in a conflict of interest.

1-3	Cybersecurity Policies and Procedures
Objective	To ensure that cybersecurity requirements are documented, communicated and complied with by the organization as per related laws and regulations, and organizational requirements.
Controls	
1-3-1	Cybersecurity policies and procedures must be defined and documented by the cybersecurity function, approved by the Authorizing Official, and disseminated to relevant parties inside and outside the organization.
1-3-2	The cybersecurity function must ensure that the cybersecurity policies and procedures are implemented.
1-3-3	The cybersecurity policies and procedures must be supported by technical security standards (e.g., operating systems, databases and firewall technical security standards).
1-3-4	The cybersecurity policies and procedures must be reviewed periodically according to planned intervals or upon changes to related laws and regulations. Changes and reviews must be approved and documented.
1-4	Cybersecurity Roles and Responsibilities
Objective	To ensure that roles and responsibilities are defined for all parties participating in implementing the cybersecurity controls within the organization.
Controls	
1-4-1	Cybersecurity organizational structure and related roles and responsibilities must be defined, documented, approved, supported and assigned by the Authorizing Official while ensuring that this does not result in a conflict of interest.
1-4-2	The cybersecurity roles and responsibilities must be reviewed periodically according to planned intervals or upon changes to related laws and regulations.
1-5	Cybersecurity Risk Management
Objective	To ensure managing cybersecurity risks in a methodological approach in order to protect the organization's information and technology assets as per organizational policies and procedures, and related laws and regulations.
Controls	
1-5-1	Cybersecurity risk management methodology and procedures must be defined, documented and approved as per confidentiality, integrity and availability considerations of information and technology assets.
1-5-2	The cybersecurity risk management methodology and procedures must be implemented by the cybersecurity function.

1-5-3	<p>The cybersecurity risk assessment procedures must be implemented at least in the following cases:</p> <p>1-5-3-1 Early stages of technology projects.</p> <p>1-5-3-2 Before making major changes to technology infrastructure.</p> <p>1-5-3-3 During the planning phase of obtaining third party services.</p> <p>1-5-3-4 During the planning phase and before going live for new technology services and products.</p>
1-5-4	The cybersecurity risk management methodology and procedures must be reviewed periodically according to planned intervals or upon changes to related laws and regulations. Changes and reviews must be approved and documented.
1-6	Cybersecurity in Information and Technology Project Management
Objective	To ensure that cybersecurity requirements are included in project management methodology and procedures in order to protect the confidentiality, integrity and availability of information and technology assets as per organization policies and procedures, and related laws and regulations.
Controls	
1-6-1	Cybersecurity requirements must be included in project and asset (information/ technology) change management methodology and procedures to identify and manage cybersecurity risks as part of project management lifecycle. The cybersecurity requirements must be a key part of the overall requirements of technology projects.
1-6-2	<p>The cybersecurity requirements in project and assets (information/technology) change management must include at least the following:</p> <p>1-6-2-1 Vulnerability assessment and remediation.</p> <p>1-6-2-2 Conducting a configurations' review, secure configuration and hardening and patching before changes or going live for technology projects.</p>
1-6-3	<p>The cybersecurity requirements related to software and application development projects must include at least the following:</p> <p>1-6-3-1 Using secure coding standards.</p> <p>1-6-3-2 Using trusted and licensed sources for software development tools and libraries.</p> <p>1-6-3-3 Conducting compliance test for software against the defined organizational cybersecurity requirements.</p> <p>1-6-3-4 Secure integration between software components.</p> <p>1-6-3-5 Conducting a configurations' review, secure configuration and hardening and patching before going live for software products.</p>
1-6-4	The cybersecurity requirements in project management must be reviewed periodically.
1-7	Compliance with Cybersecurity Standards, Laws and Regulations
Objective	To ensure that the organization's cybersecurity program is in compliance with related laws and regulations.
Controls	
1-7-1	The organization must comply with related national cybersecurity laws and regulations.
1-7-2	The organization must comply with any nationally-approved international agreements and commitments related to cybersecurity.

1-8	Periodical Cybersecurity Review and Audit
Objective	To ensure that cybersecurity controls are implemented and in compliance with organizational policies and procedures, as well as related national and international laws, regulations and agreements.
Controls	
1-8-1	Cybersecurity reviews must be conducted periodically by the cybersecurity function in the organization to assess the compliance with the cybersecurity controls in the organization.
1-8-2	Cybersecurity audits and reviews must be conducted by independent parties outside the cybersecurity function (e.g., Internal Audit function) to assess the compliance with the cybersecurity controls in the organization. Audits and reviews must be conducted independently, while ensuring that this does not result in a conflict of interest, as per the Generally Accepted Auditing Standards (GAAS), and related laws and regulations.
1-8-3	Results from the cybersecurity audits and reviews must be documented and presented to the cybersecurity steering committee and Authorizing Official. Results must include the audit/review scope, observations, recommendations and remediation plans.
1-9	Cybersecurity in Human Resources
Objective	To ensure that cybersecurity risks and requirements related to personnel (employees and contractors) are managed efficiently prior to employment, during employment and after termination/separation as per organizational policies and procedures, and related laws and regulations.
Controls	
1-9-1	Personnel cybersecurity requirements (prior to employment, during employment and after termination/separation) must be defined, documented and approved.
1-9-2	The personnel cybersecurity requirements must be implemented.
1-9-3	<p>The personnel cybersecurity requirements prior to employment must include at least the following:</p> <p>1-9-3-1 Inclusion of personnel cybersecurity responsibilities and non-disclosure clauses (covering the cybersecurity requirements during employment and after termination/separation) in employment contracts.</p> <p>1-9-3-2 Screening or vetting candidates of cybersecurity and critical/privileged positions.</p>
1-9-4	<p>The personnel cybersecurity requirements during employment must include at least the following:</p> <p>1-9-4-1 Cybersecurity awareness (during on-boarding and during employment).</p> <p>1-9-4-2 Implementation of and compliance with the cybersecurity requirements as per the organizational cybersecurity policies and procedures.</p>
1-9-5	Personnel access to information and technology assets must be reviewed and removed immediately upon termination/separation.
1-9-6	Personnel cybersecurity requirements must be reviewed periodically.

1-10	Cybersecurity Awareness and Training Program
Objective	To ensure that personnel are aware of their cybersecurity responsibilities and have the essential cybersecurity awareness. It is also to ensure that personnel are provided with the required cybersecurity training, skills and credentials needed to accomplish their cybersecurity responsibilities and to protect the organization's information and technology assets.
Controls	
1-10-1	A cybersecurity awareness program must be developed and approved. The program must be conducted periodically through multiple channels to strengthen the awareness about cybersecurity, cyber threats and risks, and to build a positive cybersecurity awareness culture.
1-10-2	The cybersecurity awareness program must be implemented.
1-10-3	<p>The cybersecurity awareness program must cover the latest cyber threats and how to protect against them, and must include at least the following subjects:</p> <ul style="list-style-type: none"> 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 use of social media.
1-10-4	<p>Essential and customized (i.e., tailored to job functions as it relates to cybersecurity) training and access to professional skillsets must be made available to personnel working directly on tasks related to cybersecurity including:</p> <ul style="list-style-type: none"> 1-10-4-1 Cybersecurity function's personnel. 1-10-4-2 Personnel working on software/application development. and information and technology assets operations. 1-10-4-3 Executive and supervisory positions.
1-10-5	The implementation of the cybersecurity awareness program must be reviewed periodically.

2 Cybersecurity Defense

2-1	Asset Management
Objective	To ensure that the organization has an accurate and detailed inventory of information and technology assets in order to support the organization's cybersecurity and operational requirements to maintain the confidentiality, integrity and availability of information and technology assets.
Controls	
2-1-1	Cybersecurity requirements for managing information and technology assets must be defined, documented and approved.
2-1-2	The cybersecurity requirements for managing information and technology assets must be implemented.
2-1-3	Acceptable use policy of information and technology assets must be defined, documented and approved.
2-1-4	Acceptable use policy of information and technology assets must be implemented.
2-1-5	Information and technology assets must be classified, labeled and handled as per related law and regulatory requirements.
2-1-6	The cybersecurity requirements for managing information and technology assets must be reviewed periodically.
2-2	Identity and Access Management
Objective	To ensure the secure and restricted logical access to information and technology assets in order to prevent unauthorized access and allow only authorized access for users which are necessary to accomplish assigned tasks.
Controls	
2-2-1	Cybersecurity requirements for identity and access management must be defined, documented and approved.
2-2-2	The cybersecurity requirements for identity and access management must be implemented.
2-2-3	<p>The cybersecurity requirements for identity and access management must include at least the following</p> <ul style="list-style-type: none"> 2-2-3-1 User authentication based on username and password. 2-2-3-2 Multi-factor authentication for remote access. 2-2-3-3 User authorization based on identity and access control principles: Need-to-Know and Need-to-Use, Least Privilege and Segregation of Duties. 2-2-3-4 Privileged access management. 2-2-3-5 Periodic review of users' identities and access rights.
2-2-4	The Implementation of the cybersecurity requirements for identity and access management must be reviewed periodically.

2-3	Information System and Information Processing Facilities Protection
Objective	To ensure the protection of information systems and information processing facilities (including workstations and infrastructures) against cyber risks.
Controls	
2-3-1	Cybersecurity requirements for protecting information systems and information processing facilities must be defined, documented and approved.
2-3-2	The cybersecurity requirements for protecting information systems and information processing facilities must be implemented.
2-3-3	<p>The cybersecurity requirements for protecting information systems and information processing facilities must include at least the following:</p> <ul style="list-style-type: none"> 2-3-3-1 Advanced, up-to-date and secure management of malware and virus protection on servers and workstations. 2-3-3-2 Restricted use and secure handling of external storage media. 2-3-3-3 Patch management for information systems, software and devices. 2-3-3-4 Centralized clock synchronization with an accurate and trusted source (e.g., Saudi Standards, Metrology and Quality Organization (SASO)).
2-3-4	The cybersecurity requirements for protecting information systems and information processing facilities must be reviewed periodically.
2-4	Email Protection
Objective	To ensure the protection of organization's email service from cyber risks.
Controls	
2-4-1	Cybersecurity requirements for protecting email service must be defined, documented and approved.
2-4-2	The cybersecurity requirements for email service must be implemented.
2-4-3	<p>The cybersecurity requirements for protecting the email service must include at the least the following:</p> <ul style="list-style-type: none"> 2-4-3-1 Analyzing and filtering email messages (specifically phishing emails and spam) using advanced and up-to-date email protection techniques. 2-4-3-2 Multi-factor authentication for remote and webmail access to email service. 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 viruses and malware. 2-4-3-5 Validation of the organization's email service domains (e.g., using Sender Policy Framework (SPF)).
2-4-4	The cybersecurity requirements for email service must be reviewed periodically.

2-5	Networks Security Management
Objective	To ensure the protection of organization's network from cyber risks.
Controls	
2-5-1	Cybersecurity requirements for network security management must be defined, documented and approved.
2-5-2	The cybersecurity requirements for network security management must be implemented.
2-5-3	<p>The cybersecurity requirements for network security management must include at least the following:</p> <ul style="list-style-type: none"> 2-5-3-1 Logical or physical segregation and segmentation of network segments using firewalls and defense-in-depth principles. 2-5-3-2 Network segregation between production, test and development environments. 2-5-3-3 Secure browsing and Internet connectivity including restrictions on the use of file storage/sharing and remote access websites, and protection against suspicious websites. 2-5-3-4 Wireless network protection using strong authentication and encryption techniques. A comprehensive risk assessment and management exercise must be conducted to assess and manage the cyber risks prior to connecting any wireless networks to the organization's internal network. 2-5-3-5 Management and restrictions on 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 viruses and malware.
2-5-4	The cybersecurity requirements for network security management must be reviewed periodically.
2-6	Mobile Devices Security
Objective	To ensure the protection of mobile devices (including laptops, smartphones, tablets) from cyber risks and to ensure the secure handling of the organization's information (including sensitive information) while utilizing Bring Your Own Device (BYOD) policy.
Controls	
2-6-1	Cybersecurity requirements for mobile devices security and BYOD must be defined, documented and approved.
2-6-2	The cybersecurity requirements for mobile devices security and BYOD must be implemented.
2-6-3	<p>The cybersecurity requirements for mobile devices security and BYOD must include at least the following:</p> <ul style="list-style-type: none"> 2-6-3-1 Separation and encryption of organization's data and information stored on mobile devices and BYODs. 2-6-3-2 Controlled and restricted use based on job requirements. 2-6-3-3 Secure wiping of organization's data and information stored on mobile devices and BYOD in cases of device loss, theft or after termination/separation from the organization. 2-6-3-4 Security awareness for mobile devices users.

2-6-4	The cybersecurity requirements for mobile devices security and BYOD must be reviewed periodically.
2-7	Data and Information Protection
Objective	To ensure the confidentiality, integrity and availability of organization's data and information as per organizational policies and procedures, and related laws and regulations.
Controls	
2-7-1	Cybersecurity requirements for protecting and handling data and information must be defined, documented and approved as per the related laws and regulations.
2-7-2	The cybersecurity requirements for protecting and handling data and information must be implemented.
2-7-3	<p>The cybersecurity requirements for protecting and handling data and information must include at least the following:</p> <p>2-7-3-1 Data and information ownership.</p> <p>2-7-3-2 Data and information classification and labeling mechanisms.</p> <p>2-7-3-3 Data and information privacy.</p>
2-7-4	The cybersecurity requirements for protecting and handling data and information must be reviewed periodically.
2-8	Cryptography
Objective	To ensure the proper and efficient use of cryptography to protect information assets as per organizational policies and procedures, and related laws and regulations.
Controls	
2-8-1	Cybersecurity requirements for cryptography must be defined, documented and approved.
2-8-2	The cybersecurity requirements for cryptography must be implemented.
2-8-3	<p>The cybersecurity requirements for cryptography must include at least the following:</p> <p>2-8-3-1 Approved cryptographic solutions standards and its technical and regulatory limitations.</p> <p>2-8-3-2 Secure management of cryptographic keys during their lifecycles.</p> <p>2-8-3-3 Encryption of data in-transit and at-rest as per classification and related laws and regulations.</p>
2-8-4	The cybersecurity requirements for cryptography must be reviewed periodically.
2-9	Backup and Recovery Management
Objective	To ensure the protection of organization's data and information including information systems and software configurations from cyber risks as per organizational policies and procedures, and related laws and regulations.
Controls	
2-9-1	Cybersecurity requirements for backup and recovery management must be defined, documented and approved.

2-9-2	The cybersecurity requirements for backup and recovery management must be implemented.
2-9-3	<p>The cybersecurity requirements for backup and recovery management must include at least the following:</p> <p>2-9-3-1 Scope and coverage of backups to cover critical technology and information assets.</p> <p>2-9-3-2 Ability to perform quick recovery of data and systems after cybersecurity incidents.</p> <p>2-9-3-3 Periodic tests of backup's recovery effectiveness.</p>
2-9-4	The cybersecurity requirements for backup and recovery management must be reviewed periodically.
2-10	Vulnerabilities Management
Objective	To ensure timely detection and effective remediation of technical vulnerabilities to prevent or minimize the probability of exploiting these vulnerabilities to launch cyber attacks against the organization.
Controls	
2-10-1	Cybersecurity requirements for technical vulnerabilities management must be defined, documented and approved.
2-10-2	The cybersecurity requirements for technical vulnerabilities management must be implemented.
2-10-3	<p>The cybersecurity requirements for technical vulnerabilities management must include at least the following:</p> <p>2-10-3-1 Periodic vulnerabilities assessments.</p> <p>2-10-3-2 Vulnerabilities classification based on criticality level.</p> <p>2-10-3-3 Vulnerabilities remediation based on classification and associated risk levels.</p> <p>2-10-3-4 Security patch management.</p> <p>2-10-3-5 Subscription with authorized and trusted cybersecurity resources for up-to-date information and notifications on technical vulnerabilities.</p>
2-10-4	The cybersecurity requirements for technical vulnerabilities management must be reviewed periodically.
2-11	Penetration Testing
Objective	To assess and evaluate the efficiency of the organization's cybersecurity defense capabilities through simulated cyber-attacks to discover unknown weaknesses within the technical infrastructure that may lead to a cyber breach.
Controls	
2-11-1	Cybersecurity requirements for penetration testing exercises must be defined, documented and approved.
2-11-2	The cybersecurity requirements for penetration testing processes must be implemented.
2-11-3	<p>The cybersecurity requirements for penetration testing processes must include at least the following:</p> <p>2-11-3-1 Scope of penetration tests which must cover Internet-facing services and its technical components including infrastructure, websites, web applications, mobile apps, email and remote access.</p> <p>2-11-3-2 Conducting penetration tests periodically.</p>

2-11-4	Cybersecurity requirements for penetration testing processes must be reviewed periodically.
2-12	Cybersecurity Event Logs and Monitoring Management
Objective	To ensure timely collection, analysis and monitoring of cybersecurity events for early detection of potential cyber-attacks in order to prevent or minimize the negative impacts on the organization's operations.
Controls	
2-12-1	Cybersecurity requirements for event logs and monitoring management must be defined, documented and approved.
2-12-2	The cybersecurity requirements for event logs and monitoring management must be implemented.
2-12-3	<p>The cybersecurity requirements for event logs and monitoring management must include at least the following:</p> <p>2-12-3-1 Activation of cybersecurity event logs on critical information assets.</p> <p>2-12-3-2 Activation of cybersecurity event logs on remote access and privileged user accounts.</p> <p>2-12-3-3 Identification of required technologies (e.g., SIEM) for cybersecurity event logs collection.</p> <p>2-12-3-4 Continuous monitoring of cybersecurity events.</p> <p>2-12-3-5 Retention period for cybersecurity event logs (must be 12 months minimum).</p>
2-12-4	The cybersecurity requirements for event logs and monitoring management must be reviewed periodically.
2-13	Cybersecurity Incident and Threat Management
Objective	To ensure timely identification, detection, effective management and handling of cybersecurity incidents and threats to prevent or minimize negative impacts on organization's operation taking into consideration the Royal Decree number 37140, dated 14/8/1438H.
Controls	
2-13-1	Requirements for cybersecurity incidents and threat management must be defined, documented and approved.
2-13-2	The requirements for cybersecurity incidents and threat management must be implemented.
2-13-3	<p>The requirements for cybersecurity incidents and threat management must include at least the following:</p> <p>2-13-3-1 Cybersecurity incident response plans and escalation procedures.</p> <p>2-13-3-2 Cybersecurity incidents classification.</p> <p>2-13-3-3 Cybersecurity incidents reporting to NCA.</p> <p>2-13-3-4 Sharing incidents notifications, threat intelligence, breach indicators and reports with NCA.</p> <p>2-13-3-5 Collecting and handling threat intelligence feeds.</p>
2-13-4	The requirements for cybersecurity incidents and threat management must be reviewed periodically.

2-14	Physical Security
Objective	To ensure the protection of information and technology assets from unauthorized physical access, loss, theft and damage.
Controls	
2-14-1	Cybersecurity requirements for physical protection of information and technology assets must be defined, documented and approved.
2-14-2	The cybersecurity requirements for physical protection of information and technology assets must be implemented.
2-14-3	<p>The cybersecurity requirements for physical protection of information and technology assets must include at least the following:</p> <p>2-14-3-1 Authorized access to sensitive areas within the organization (e.g., data center, disaster recovery center, sensitive information processing facilities, security surveillance center, network cabinets).</p> <p>2-14-3-2 Facility entry/exit records and CCTV monitoring.</p> <p>2-14-3-3 Protection of facility entry/exit and surveillance records.</p> <p>2-14-3-4 Secure destruction and re-use of physical assets that hold classified information (including documents and storage media).</p> <p>2-14-3-5 Security of devices and equipment inside and outside the organization's facilities.</p>
2-14-4	The cybersecurity requirements for physical protection of information and technology assets must be reviewed periodically.
2-15	Web Application Security
Objective	To ensure the protection of external web applications against cyber risks.
Controls	
2-15-1	Cybersecurity requirements for external web applications must be defined, documented and approved.
2-15-2	The cybersecurity requirements for external web applications must be implemented.
2-15-3	<p>The cybersecurity requirements for external web applications must include at least the following:</p> <p>2-15-3-1 Use of web application firewall.</p> <p>2-15-3-2 Adoption of the multi-tier architecture principle.</p> <p>2-15-3-3 Use of secure protocols (e.g., HTTPS).</p> <p>2-15-3-4 Clarification of the secure usage policy for users.</p> <p>2-15-3-5 Multi-factor authentication for users' access.</p>
2-15-4	The cybersecurity requirements for external web applications must be reviewed periodically.

3 Cybersecurity Resilience

3-1	Cybersecurity Resilience Aspects of Business Continuity Management (BCM)
Objective	To ensure the inclusion of the cybersecurity resiliency requirements within the organization's business continuity management and to remediate and minimize the impacts on systems, information processing facilities and critical e-services from disasters caused by cybersecurity incidents.
Controls	
3-1-1	Cybersecurity requirements for business continuity management must be defined, documented and approved.
3-1-2	The cybersecurity requirements for business continuity management must be implemented.
3-1-3	<p>The cybersecurity requirements for business continuity management must include at least the following:</p> <ul style="list-style-type: none">3-1-3-1 Ensuring the continuity of cybersecurity systems and procedures.3-1-3-2 Developing response plans for cybersecurity incidents that may affect the business continuity.3-1-3-3 Developing disaster recovery plans.
3-1-4	The cybersecurity requirements for business continuity management must be reviewed periodically.



Third-Party and Cloud Computing Cybersecurity

4-1	Third-Party Cybersecurity
Objective	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.
Controls	
4-1-1	Cybersecurity requirements for contracts and agreements with third-parties must be identified, documented and approved.
4-1-2	<p>The cybersecurity requirements for contracts and agreements with third-parties (e.g., Service Level Agreement (SLA)) -which may affect, if impacted, the organization's data or services- must include at least the following:</p> <p>4-1-2-1 Non-disclosure clauses and secure removal of organization's data by third parties upon end of service.</p> <p>4-1-2-2 Communication procedures in case of cybersecurity incidents.</p> <p>4-1-2-3 Requirements for third-parties to comply with related organizational policies and procedures, laws and regulations.</p>
4-1-3	<p>The cybersecurity requirements for contracts and agreements with IT outsourcing and managed services third-parties must include at least the following:</p> <p>4-1-3-1 Conducting a cybersecurity risk assessment to ensure the availability of risk mitigation controls before signing contracts and agreements or upon changes in related regulatory requirements.</p> <p>4-1-3-2 Cybersecurity managed services centers for monitoring and operations must be completely present inside the Kingdom of Saudi Arabia.</p>
4-1-4	The cybersecurity requirements for contracts and agreements with third-parties must be reviewed periodically.
4-2	Cloud Computing and Hosting Cybersecurity
Objective	To ensure the proper and efficient remediation of cyber risks and the implementation of cybersecurity requirements related to hosting and cloud computing as per organizational policies and procedures, and related laws and regulations. It is also to ensure the protection of the organization's information and technology assets hosted on the cloud or processed/managed by third-parties.
Controls	
4-2-1	Cybersecurity requirements related to the use of hosting and cloud computing services must be defined, documented and approved.
4-2-2	The cybersecurity requirements related to the use of hosting and cloud computing services must be implemented.

4-2-3	<p>In line with related and applicable laws and regulations, and in addition to the applicable ECC controls from main domains (1), (2), (3) and subdomain (4-1), the cybersecurity requirements related to the use of hosting and cloud computing services must include at least the following:</p> <p>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.</p> <p>4-2-3-2 Separation of organization's environments (specifically virtual servers) from other environments hosted at the cloud service provider.</p> <p>4-2-3-3 Organization's information hosting and storage must be inside the Kingdom of Saudi Arabia.</p>
4-2-4	<p>The cybersecurity requirements related to the use of hosting and cloud computing services must be reviewed periodically.</p>



Industrial Control Systems Cybersecurity

5-1	Industrial Control Systems (ICS) Protection
Objective	To ensure the appropriate and effective cybersecurity management of Industrial Controls Systems and Operational Technology (ICS/OT) to protect the confidentiality, integrity and availability of the organization's assets against cyber attacks (e.g., unauthorized access, destruction, spying and fraud) in line with the organization's cybersecurity strategy and related and applicable local and international laws and regulations.
Controls	
5-1-1	Cybersecurity requirements related to Industrial Controls Systems and Operational Technology (ICS/OT) must be defined, documented and approved.
5-1-2	The cybersecurity requirements related to Industrial Controls Systems and Operational Technology (ICS/OT) must be implemented.
5-1-3	<p>In addition to the applicable ECC controls from the main domains (1), (2), (3) and (4), the cybersecurity requirements related to Industrial Controls Systems and Operational Technology (ICS/OT) must include at least the following:</p> <ul style="list-style-type: none"> 5-1-3-1 Strict physical and virtual segmentation when connecting industrial production networks to other networks within the organization (e.g., corporate network). 5-1-3-2 Strict physical and virtual segmentation when connecting systems and industrial networks with external networks (e.g., Internet, wireless, remote access). 5-1-3-3 Continuous monitoring and activation of cybersecurity event logs on the industrial networks and its connections. 5-1-3-4 Isolation of Safety Instrumental Systems (SIS). 5-1-3-5 Strict limitation on the use of external storage media. 5-1-3-6 Strict limitation on connecting mobile devices to industrial production networks. 5-1-3-7 Periodic review and secure configuration and hardening of industrial, automated, support systems, and devices. 5-1-3-8 Vulnerability management for industrial control systems and operational technology (ICS/OT). 5-1-3-9 Patch management for industrial control systems and operational technology (ICS/OT). 5-1-3-10 Cybersecurity applications management related to the protection of the industrial systems from viruses and malware.
5-1-4	The cybersecurity requirements related to Industrial Controls Systems and Operational Technology (ICS/OT) must be reviewed periodically.

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 Definitions

Terminology	Definition
Advanced Persistent Threat (APT) Protection	Protection against advanced threats that use invisible techniques to gain unauthorized access to systems and networks and stay as long as possible through circumventing detection and protection tools. To accomplish that, viruses and zero-day malware are used in these techniques.
Asset	Anything tangible or intangible that has value to the organization. There are many types of assets, and some of which include obvious things, such as: persons, machineries, utilities, patents, software and services. The term could also include less obvious things, such as: information and characteristics (e.g., organization's reputation and public image, as well as skill and knowledge).
Attack	Any kind of malicious activity that attempts to achieve unauthorized access, collection, disabling, prevention, destroy or sabotage of the information system resources or the information itself.
Audit	Independent review and examination of records and activities to assess the effectiveness of cybersecurity controls and to ensure compliance with established policies, operational procedures and relevant standard, legal and regulatory requirements.
Authentication	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in a system.
Authorization	It is the function of defining and verifying access rights/privileges to resources related to organization's information and technical assets security in general and to access control in particular.
Availability	Ensuring timely access to 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 the policy of the organization that allows (in part or in whole) its employees to bring their personal devices (laptops, tablets and smartphones) to the premises of the organization and use such devices to access the networks, information, applications and systems of the organization which are access-restricted.
Change Management	It is a service management system that ensures a systematic and proactive approach using effective standard methods and procedures (e.g., change in infrastructure and networks). Change Management helps all stakeholders, including individuals and teams alike, move from their current state to the next desired state, and also helps reduce the impact of relevant incidents on service.

Terminology	Definition
Closed-Circuit Television CCTV	Closed-Circuit Television (CCTV), also known as video surveillance, is the use of video cameras to transmit a signal to a specific place, on a limited set of monitors. The term is often applied to those used for surveillance in areas that may need monitoring where physical security is needed.
Cloud Computing	<p>A model for enabling on-demand network access to a shared pool of configurable IT capabilities/resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal operation management effort or service provider interaction. It allows users to access technology-based services from the cloud without knowledge of, expertise with, or control over the technology infrastructure that supports them.</p> <p>The cloud computing model is composed of five essential characteristics: on-demand self-service, ubiquitous network access, location independent resource pooling, rapid elasticity and measured service. There are three types of cloud computing services delivery models: Cloud Software as a Service (SaaS), Cloud Platform as a Service (PaaS), and Cloud Infrastructure as a Service (IaaS);</p> <p>Based on the enterprise access for cloud computing, there are four models: Private Cloud, Community Cloud, Public Cloud, and Hybrid Cloud.</p>
Compromise	<p>Disclosure of or obtaining information by unauthorized persons, which are unauthorized to be leaked or obtained, or violation of the cybersecurity policy of the organization through disclosure, change, sabotage or loss of anything, either intentionally or unintentionally.</p> <p>The expression "compromise" means disclosure of, obtaining, leaking, altering or use of sensitive data without authorization (including cryptographic keys and other critical cybersecurity standards).</p>
Confidential Data/Information	<p>Organizational information (or data) that is considered highly critical and sensitive as per the organization's data classification, which it has prepared to be used by the organization itself or other specific organizations. One way to determine the classification of such type of information/data is through assessing the impact from unauthorized disclosure, access, loss or damage. Impacts could be financial or reputational on the organization or customers, impact on the lives of people related to the disclosed information, impact and harm on the national security, economy or capabilities.</p> <p>Confidential Data/Information includes all information that if disclosed, lost or damaged in an unauthorized manner, there would be legal consequences.</p>
Confidentiality	Maintaining authorized restrictions on access to and disclosure of information, including means of protecting privacy/personal information.
Critical National Infrastructure (CNI)	<p>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:</p> <ul style="list-style-type: none"> • 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.

Terminology	Definition
Cryptography	These are the 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, prevent unauthorized use or prevent undetected modification so that only the persons concerned can read and process the same.
Cyber Attack	Intentional exploitation of computer systems, networks, and organizations whose work depends on digital ICT, in order to cause damage.
Cyber Risks	The risks to organizational operations (including vision, mission, functions, image or reputation), organizational assets, individuals, other organizations, or the nation due to the potential of unauthorized access, use, disclosure, disruption, modification, or destruction of information and/or information systems.
Cybersecurity	According to the Royal Decree number 6801, dated 11/2/1439H, cybersecurity is the protection of networks, IT systems, operational technologies systems and their components of hardware and software, their services and the data they contain, from any penetration, disruption, modification, access, use or unauthorized exploitation. The concept of cybersecurity also includes information security and digital security.
Cybersecurity Resilience	The overall ability of organizations to withstand cyber events and, where harm is caused, recover from them.
Cyberspace	The interconnected network of IT infrastructure, including the Internet, communications networks, computer systems and Internet-connected devices, as well as the associated hardware and control devices. The term can also refer to a virtual world or domain such as a simple concept.
Data and Information Classification	Setting the sensitivity level of data and information that results in security controls for each level of classification. 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 indication of the value or importance of the data and information of the organization.
Data Archiving	It is the process of moving 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 organization and may be needed for future reference, as well as data that must be retained for relevant legal and regulatory compliance.
Defense-in-Depth	It is an information assurance concept in which multiple layers of security controls (defense) are placed throughout an information technology (IT) or operation technology (OT) system.
Disaster Recovery	Programs, activities and plans designed to restore the organization's critical business functions and services to an acceptable situation, following exposure to cyber attacks or disruption of such services.
Domain Name System (DNS)	A technical system that uses a database distributed over the network and/or the Internet which allows the translation of domain names into IP addresses, and vice-versa in order to identify service addresses such as web and email servers.

Terminology	Definition
Effectiveness	Effectiveness refers to the degree to which a planned impact is achieved. Planned activities are considered effective if these activities are already implemented, and the planned results are considered effective if the results are already achieved. KPIs can be used to measure and evaluate the level of effectiveness.
Efficiency	The 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	Something that happens in a specific place (such as network, systems, applications) at a specific time.
Hyper Text Transfer Protocol Secure (HTTPS)	A protocol that uses encryption to secure web pages and data when they are transmitted over the network. It is a secure version of the Hypertext Text Transfer Protocol (HTTP).
Identification	It is the means of verifying the identity of a user, process, or device, typically as a prerequisite for granting access to resources in a system.
Incident	A compromise through violation of cybersecurity policies, acceptable use policies, practices or cybersecurity controls or requirements.
Integrity	Protection against unauthorized modification or destruction of information, including ensuring information non-repudiation and authenticity.
(Inter) National Requirements	National requirements are those developed by a regulatory organization or body in Saudi Arabia for regulatory use (e.g., NCA's Essential Cybersecurity Controls ECC-1:2018) International requirements are those developed by a global organization for worldwide regulatory or best practices use (e.g., SWIFT, PCI DSS).
Intrusion Prevention System (IPS)	A system with intrusion detection capabilities, as well as the ability to prevent and stop suspicious or potential incidents.
Key Performance Indicator (KPI)	A type of performance measurement that evaluates the success of an organization or of a particular activity in which it engages to achieve particular objectives and goals.
Labelling	Display of information (by specific and standard naming and coding) that is placed on the organization's assets (such as devices, applications and documents) to be used to refer to some information related to the classification, ownership, type and other asset management information.
Least Privilege	A basic principle in cybersecurity that aims at granting users the access privileges they need to carry out their official responsibilities only.
Malware	A program that infects systems, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or of otherwise annoying or disrupting the victim.
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: <ul style="list-style-type: none"> • 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 (a characteristic of the user only, such as fingerprint).

Terminology	Definition
Multi-tier Architecture	An architecture or structure to which a client-server approach is applied, 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	The restriction of data, which is considered sensitive unless one has a specific need to know; for official business duties.
Offline/Offsite Backup	A backup of databases, settings, systems, applications and devices in which it is offline and not accessible to update. Typically, backup tapes are utilized for offsite backup.
Online Backup	A method of storage in which the backup is regularly taken on a remote server over a network, (either within the organization's network or hosted by a service provider).
Organization Staff	Individuals who work for the organization (including employees, temporary employees and contractors).
Outsourcing	Obtaining goods or services by contracting with a supplier or service provider.
Patch	Supporting data pack used to upgrade, fix or improve computer operating systems, software or applications. This includes fixing security vulnerabilities and other bugs, with such patches usually called fixes or bug fixes and system usability or performance improvement.
Penetration Testing	The practice of testing a computer system, network, web application or mobile application to find vulnerabilities that an attacker could exploit.
Phishing Emails	The attempt to obtain sensitive information such as usernames, passwords, or credit card details, often for malicious reasons and intentions, by disguising as a trustworthy organization in email messages.
Physical Security	Physical security describes security measures designed to prevent unauthorized access to the Organization's facilities, equipment and resources, and to protect individuals and property from damage or harm (such as espionage, theft or terrorist attacks). Physical security involves the use of multiple-tier of interconnected systems, including CCTV, security guards, security limits, locks, access control systems and many other technologies.
Policy	A document whose statements define a general commitment, direction, or intention of an organization as formally expressed by its Authorizing Official. Cybersecurity policy is a document whose statements express management's formal commitment to the implementation and improvement of the organization's cybersecurity program and include the organization's objectives regarding the cybersecurity and its controls and requirements, and the mechanisms for improving and developing it.
Privacy	Freedom from unauthorized interference or disclosure of personal information about an individual.
Privileged Access Management	The process of managing high-risk privileges on systems which need special handling to minimize risk that may arise from rights misuse.
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 can be a subset of processes.
Process	A set of interrelated or interactive activities that translated input into output. Such activities are influenced by the policies of the organization.
Recovery	A procedure or process to restore or control something that is suspended, damaged, stolen or lost.

Terminology	Definition
Retention	The length of time that information, data, event logs or backups must be retained, regardless of the form (i.e., paper and electronic).
Secure Coding Standards	A practice for the development of computer software and applications in a way that protects against the exposure to cybersecurity vulnerabilities related to software and applications.
Secure Configuration and Hardening	Protecting, hardening and configuring the settings of computers, systems, applications, network devices and security devices for resisting cyber-attacks, such as: stopping or changing factory and default accounts, stopping of unused services and unused network ports.
Security Information and Event Management (SIEM)	A system that manages and analyzes security events logs in real time in order to provide monitoring of threats, analysis of the results of interrelated rules for event logs and reports on logs data, and incident response.
Security Testing	A process intended to ensure that modified or new systems and applications include appropriate security controls and protection and do not introduce any security holes or vulnerabilities that might compromise other systems or applications or misuses of the system, application or its information, and to maintain functionality as intended.
Security-by-Design	A methodology to systems and software development and networks design that seeks to make systems, software and networks free from cybersecurity vulnerabilities/weaknesses and impervious to cyber-attack as much as possible through measures such as: continuous testing, authentication safeguards and adherence to best programming and design practices.
Sender Policy Framework	A method to validate that the email server used in the sender's email address actually belongs to the sender's organization email domain.
Segregation of Duties	Key principle in cybersecurity that aims at minimizing errors and fraud when processing specific tasks. It is accomplished through having several people with different privileges, required to complete a task.
Third-Party	Any organization acting as a party in a contractual relationship to provide goods or services (this includes suppliers and service providers).
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 particular information system vulnerability.
Threat Intelligence	It provides organized information and analysis of recent, current and potential attacks that could pose a cyber threat to the organization.
Vulnerability	Any type of weakness in a computer system, software, application, set of procedures, or in anything that leaves cybersecurity exposed to a threat.
Web Application Firewall	It analyzes, filters, monitors, and blocks Internet traffic to and from a web application. It is also able to filter the content of specific web applications.
Zero-Day Malware	Malware that is unknown before, produced/disseminated recently, and normally hard to detect by signature-based protection anti-malware applications.

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

Abb.	Full Term
APT	Advanced Persistent Threat
BCM	Business Continuity Management
BYOD	Bring Your Own Device
CCTV	Closed-Circuit Television
CNI	Critical National Infrastructure
DNS	Domain Name System
ECC	Essential Cybersecurity Controls
HTTPS	Hyper Text Transfer Protocol Secure
ICS	Industrial Control System
ICT	Information and Communication Technology
IT	Information Technology
MFA	Multi-Factor Authentication
OT	Operational Technology
SIEM	Security Information and Event Management
SIS	Safety Instrumented System
SLA	Service Level Agreement



الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

