الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

Draft Non-CNI Private Sector Organizations Cybersecurity Controls

(NCNICC – 1:2024)

Public Consultation Version

TLP: White

Document Classification: Public

Public Consultation Version

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.

Public Consultation Version

In the Name of Allah,

The Most Gracious,

The Most Merciful

Public Consultation Version

Traffic Light Protocol (TLP):

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

Red – Personal, Confidential, and for the 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

Public Consultation Version

Table of Contents

INTRODUCTION 10
OBJECTIVES 11
SCOPE OF WORK AND APPLICABILITY 12
NCNICC SCOPE OF WORK 12
NCNICC STATEMENT OF APPLICABILITY 13
IMPLEMENTATION AND COMPLIANCE 14
UPDATE AND REVIEW 14
NCNICC ORGANIZATION SEGMENTS 15
NCNICC DOMAINS AND STRUCTURE 15
MAIN DOMAINS 15
SUBDOMAINS 16
STRUCTURE 17
NON-CNI PRIVATE SECTOR ORGANIZATIONS CYBERSECURITY CONTROLS 19
APPENDIX 28

List of Tables

TABLE 1: NCNICC DOMAINS, SUBDOMAINS, & CONTROLS 10
TABLE 2: NCNICC ORGANIZATION SEGMENTS 12
TABLE 3: NCNICC SUBDOMAINS 16
TABLE 4: NCNICC STRUCTURE 17
TABLE 5: NCNICC CONTROL APPLICABILITY LEGEND 18
TABLE 6: TERMS & DEFINITIONS 28
TABLE 7: LIST OF ABBREVIATIONS 33

List of Figures

FIGURE 1: MAIN DOMAINS FOR NCNICC 15
FIGURE 2: CONTROLS CODING SCHEME 17
FIGURE 3: NCNICC STRUCTURE 17

Public Consultation Version

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 aimed at strengthening the private sector and increasing the contribution of the private sector to 65% of GDP. Vision 2030 is also targeting an increase in small and medium organization's contribution to 35% of GDP. Small, medium, and large organizations therefore figure prominently in these economic goals. With the goal of such ambitious growth, it is imperative that organizations in the Kingdom of Saudi Arabia are held to this common standard, to improve cybersecurity resilience within the private sector. The Non-CNI Private Sector Organizations Cybersecurity Controls (NCNICC) are focused on the private sector (small, medium and large organizations) since they represent a critical part of supporting the realization of the Kingdom's economic goals.

The NCA's Mandate, as per Royal Order 6801 dated 11/2/1439H, states that the NCA is the cybersecurity regulator in the kingdom and the national reference for all cybersecurity matters. NCA's mandate and duties fulfill the strategic and regulatory cybersecurity needs related to the development of cybersecurity national policies, governance mechanisms, frameworks, standards, and controls and guidelines. The NCA's mandate and duties also fulfill the need to continuously monitor the compliance of organizations to support the important role of cybersecurity, the importance of which has only increased in recent years with the rise of security risks in cyberspace.

Public Consultation Version

NCA's mandate for cybersecurity covers all government, private, and other organizations in the Kingdom. In order to achieve a secure and trusted Saudi cyberspace that enables growth and prosperity, NCA has developed the Non-CNI Private Sector Organizations Cybersecurity Controls (NCNICC-1:2024). The NCNICC set the cybersecurity controls for small, medium, and large organizations operating in the Kingdom. This document highlights the objectives of the controls, along with details on each, their scope, statement of applicability, compliance approach and monitoring.

The Non-CNI Private Sector Organizations Cybersecurity Controls are organized into three domains: Cybersecurity Governance, Cybersecurity Defense, and Third Party Cybersecurity.

Public Consultation Version

Introduction

The NCA developed the Non-CNI Private Sector Organizations Cybersecurity Controls (NCNICC-1:2024) after conducting a comprehensive study of the small, medium and large organizations' cybersecurity regulations and standards that national and international organizations have developed. In addition, the NCNICC was developed in alignment with the Essential Cybersecurity Controls (ECC) to provide a more suitable version for organizations in scope of work.

The Non-CNI Private Sector Organizations Cybersecurity Controls apply to two organizational segments; small & medium, and large organizations, as defined in Table 1. The Non-CNI Private Sector Organizations Cybersecurity Controls consist of the following:

Organization Segment	Number of Required Domains, Subdomains & Controls
Segment 1 (S1): Large Organizations	• 2 Main domains • 15 Subdomains • 27 Main controls
Segment 2 (S2): Small and Medium Organizations	• 1 Main domain • 7 Subdomains • 7 Main controls

Table 1: NCNICC Domains, Subdomains, & Controls

Public Consultation Version

Objectives

The main objective of this document is to set the minimum cybersecurity controls for non-CNI. The controls are based on industry leading practices which will help non-CNI 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 three main cybersecurity pillars:

- People
- Processes
- Technology

Public Consultation Version

Scope of Work and Applicability

NCNICC Scope of Work

The NCNICC are targeted at all small, medium and large private organizations (excluding private sector organizations owning, operating or hosting Critical National Infrastructure (CNIs)) in the Kingdom of Saudi Arabia.

The Non-CNI Private Sector Organizations Cybersecurity Controls are targeting two organization segments: Segment 1 (Large Organizations) and Segment 2 (Small and Medium Organizations). The segments in NCNICC are based on the size of the organization, and are aligned with the definitions of small, medium and large organizations by Small and Medium Enterprises General Authority (Monsha'at). Table 2 below illustrates the NCNICC organization segments.

Organization Segment	Definition	Number of Required Domains, Subdomains, & Controls
Segment 1 (S1): Large Organizations	Large organizations refer to organizations that employ more than 250 employees or generate more than 200 million SAR in annual revenue.	• 2 domains • 15 subdomains • 27 controls
Segment 2 (S2): Small and Medium Organizations	Small and medium organizations refer to organizations that employ between 6 to 249 employees or generate between 3 to 200 million SAR in annual revenue.	• 1 domain • 7 subdomains • 7 controls

Table 2: NCNICC Organization Segments

Segment 1 controls are mandatory for large organizations, whereas Segment 2 controls are mandatory for small and medium organizations. NCA strongly encourages small and medium organizations in the Kingdom to leverage Segment 1 controls to implement best practices to improve and enhance their cybersecurity maturity.

The NCA strongly encourages all other organizations outside the scope of work NCA controls (such as micro-organizations and Non-Governmental Organizations (NGOs)) in the Kingdom to leverage these controls to implement best practices to improve and enhance their cybersecurity posture.

NCNICC Statement of Applicability

The NCNICC controls were developed taking into consideration the cybersecurity needs of small, medium, and large organizations in the Kingdom of Saudi Arabia.

Applicability to implement these cybersecurity controls depends on the organization's segment type as defined in Table 2. For example:

- Controls in subdomain 2-3 (Information System and Information Processing Facilities Protection) are applicable and must be implemented by large organizations (Segment 1) as well as small and medium organizations (Segment 2).
- Controls in subdomain 2-1 (Asset Management) are applicable and must be implemented by large organizations (Segment 1).

Public Consultation Version

Implementation and Compliance

To comply with item 3 of article 10 of NCA's mandate, all organizations within the scope of these controls must implement whatever necessary to ensure continuous compliance with the controls. NCA reserves the right to, at its discretion, carry out audits on an organization's compliance with the applicable controls.

NCA evaluates the organization's compliance with the NCNICC through multiple means, such as external assessments by an NCA licensed compliance assessment service provider, in accordance with mechanisms deemed appropriate by NCA.

Update and Review

NCA will periodically review and update the NCNICC as per the cybersecurity requirements and related industry changes. NCA will communicate and publish the updated version of NCNICC for implementation and compliance.

Public Consultation Version

NCNICC Domains and Structure

Main Domains

Figure 1 below shows the main domains of NCNICC.



Figure 1: Main Domains for NCNICC

Public C

Subdomains

Table 3 below shows the NCNICC subdomains.

1. Cybersecurity Governance	1-1	Cybersecurity Management	1-2	Cybersecurity Policies and Procedures
	1-3	Periodical Cybersecurity Review and Audit	1-4	Cybersecurity Awareness and Training Program
2. Cybersecurity Defense	2-1	Asset Management	2-2	Identity and Access Management
	2-3	Information System and Information Processing Facilities Protection	2-4	Email Protection
	2-5	Networks Security Management	2-6	Cryptography
	2-7	Backup and Recovery Management	2-8	Vulnerabilities Management
	2-9	Penetration Testing	2-10	Cybersecurity Event Logs and Monitoring Management
	2-11	Cybersecurity Incident and Threat Management	2-12	Physical Security
3. Third-Party Cybersecurity	3-1	Third-Party Cybersecurity		

Table 3: NCNICC Subdomains

Public Consultation Version

Structure

Figures 2 and 3 below show the meaning of controls codes.

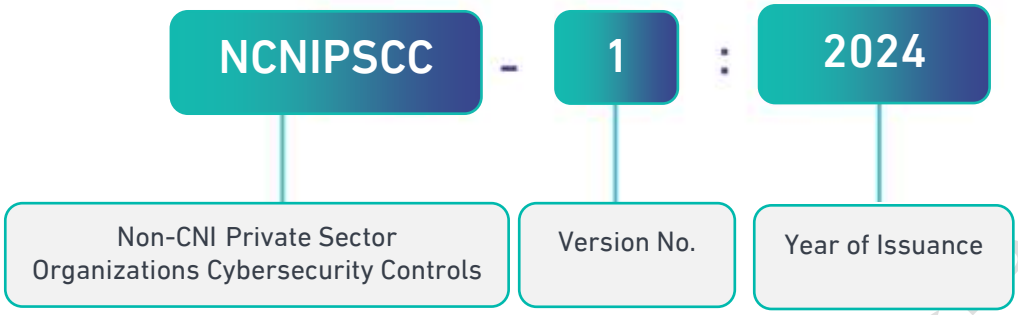


Figure 2: Controls Coding Scheme

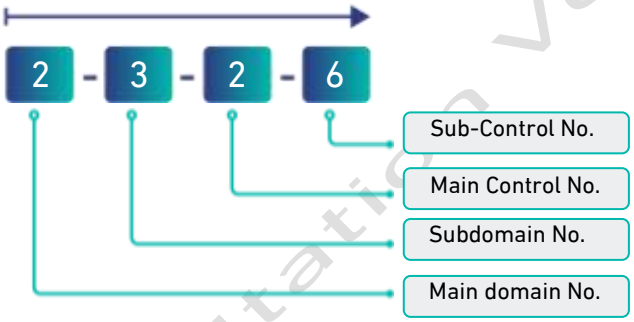


Figure 3: NCNICC Structure

1		Name of Main Domain	
Reference Number of the Main Domain			
Reference No. of the Subdomain		Name of Subdomain	
Objective			
Controls		Control Applicability	
		S1	S2
Control Reference Number	Control Clauses		

Table 4: NCNICC Structure

Consultation version

Control applicability depends on the organization's segment, and is indicated for each control as shown in Table 5.

Control Applicability	Description
Required	Control mandatory for the organization segment or contains one or more sub-controls that are mandatory for the organization segment.
Recommended	Control is not mandatory for the organization segment, however organizations are encouraged to apply the control.

Table 5: NCNICC Control Applicability Legend

Public Consultation Version

Non-CNI Private Sector Organizations Cybersecurity Controls



Cybersecurity Governance

1-1	Cybersecurity Management		
Objective	To ensure leadership support in implementing and managing cybersecurity programs within the organization.		
Controls		Control Applicability	
		S1	S2
1-1-1	A cybersecurity function/role must be established within the organization. This function/role must be independent from the IT function.	Required	Recommended
1-2	Cybersecurity Policies and Procedures		
Objective	To ensure that cybersecurity requirements are documented, communicated, and complied with by the organization.		
Controls		Control Applicability	
		S1	S2
1-2-1	Cybersecurity policies for employees must be defined, documented, approved, disseminated to employees (e.g., cybersecurity policy).	Required	Recommended
1-2-2	The cybersecurity function/role must ensure that the cybersecurity policies are implemented.	Required	Recommended
1-3	Periodical Cybersecurity Review and Audit		
Objective	To ensure that cybersecurity controls are implemented and in compliance with organizational policies and procedures, where applicable, as well as related national NCA issued and international laws, regulations and agreements.		
Controls		Control Applicability	
		S1	S2

1-3-1	Cybersecurity audits and reviews must be conducted by an NCA licensed compliance assessment service provider, to assess the compliance with the NCNICC (as per the required frequency).	Required (every 3 years)	Recommended
1-4	Cybersecurity Awareness and Training Program		
Objective	To ensure that personnel are aware of their cybersecurity responsibilities and have the essential cybersecurity awareness.		
Controls		Control Applicability	
		S1	S2
1-4-1	The cybersecurity awareness programs must cover key relevant topics (e.g., phishing, ransomware, strong passwords, safe behavior on social media, reporting incidents and suspicious behavior) and must be tailored to the roles and needs of employees.	Required	Recommended
1-4-2	The cybersecurity awareness program must be implemented.	Required	Recommended



Cybersecurity Defense

2-1	Asset Management		
Objective	To ensure that the organization has an accurate 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		Control Applicability	
		S1	S2
2-1-1	Cybersecurity requirements for managing information and technology assets must be defined, documented and approved.	Required	Recommended

Public Consultation

2-1-2	The cybersecurity requirements for managing information and technology assets must be implemented.	Recommended	Recommended
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		Control Applicability	
		S1	S2
2-2-1	Cybersecurity requirements for identity and access management must be defined, documented, approved and must include at least the following:	Required	Required
	2-2-1-1 User authentication based on username and strong password.	Required	Required
	2-2-1-2 Multi-factor authentication for remote access and external applications.	Required	Recommended
	2-2-1-3 User authorization based on identity and access control principles: Need-to-Know, Need-to-Use, Least Privilege and Segregation of Duties.	Required	Recommended
	2-2-1-4 Privileged access management.	Required	Recommended
	2-2-1-5 Periodic review of users' identities and access rights.	Required	Recommended
2-2-2	The cybersecurity requirements for identity and access management must be implemented.	Required	Recommended
2-3	Information System and Information Processing Facilities Protection		
Objective	To ensure the protection of information systems and information processing facilities (including workstations, servers, and network devices) against cyber risk.		
Controls		Control Applicability	
		S1	S2

Public Consultation Version

2-3-1	Cybersecurity requirements for protecting information systems and information processing facilities must be defined, documented, approved and must include at least the following:	Required	Required
	2-3-1-1 Up-to-date and secure management (e.g., automated scans, automatic updates) of malware and virus protection on servers, workstations and mobile devices.	Required	Required
	2-3-1-2 Change of default/weak configurations (e.g., deactivation of unneeded services, change of default passwords, restricted use of removable media).	Required	Required
2-3-2	The cybersecurity requirements for protecting information systems and information processing facilities must be implemented.	Required	Required
2-4	Email Protection		
Objective	To ensure the protection of organization's email service from cyber risks.		
Controls		Control Applicability	
		S1	S2
2-4-1	Cybersecurity requirements for protecting email service must be defined, documented, approved and must include at the least the following:	Required	Recommended
	2-4-1-1 Analyzing and filtering email messages (specifically phishing emails and spam) using up-to-date email protection techniques.	Required	Recommended
	2-4-1-2 Validation of the organization's email service domains through Haseen platform by using Sender Policy Framework (SPF), Domain Keys Identified Mail (DKIM), and Domain Message Authentication Reporting and Conformance (DMARC).	Required	Recommended
2-4-2	The cybersecurity requirements for email service must be implemented.	Required	Recommended
2-5	Networks Security Management		
Objective	To ensure the protection of organization's network from cyber risks.		

Public Consultation Version

Controls		Control Applicability	
		S1	S2
2-5-1	Cybersecurity requirements for network security management must be defined, documented, approved, and must include at least the following:	Required	Required
	2-5-1-1 Use of network firewalls and secure access gateways.	Required	Required
	2-5-1-2 Logical or physical segregation and segmentation of network segments.	Recommended	Recommended
	2-5-1-3 Wireless network protection using strong authentication and encryption techniques.	Required	Required
2-5-2	The cybersecurity requirements for network security management must be implemented.	Required	Recommended
2-6	Cryptography		
Objective	To ensure the proper and efficient use of cryptography to protect information assets.		
Controls		Control Applicability	
		S1	S2
2-6-1	Cybersecurity requirements for cryptography must be defined, documented, approved and must include at least the following:	Required	Recommended
	2-6-1-1 Use of encryption of data at-rest and in-transit.	Recommended	Recommended
	2-6-1-2 Use secure and up-to-date cryptographic methods and algorithms when creating, storing, transmitting data, and for overall network communication medium; as per the requirements of the "moderate level" in the National Cryptographic Standards (NCS-1:2020).	Required	Recommended
2-6-2	The cybersecurity requirements for cryptography must be implemented.	Required	Recommended

Public Consultation Version

2-7	Backup and Recovery Management		
Objective	To ensure the protection of organization's data and information including information systems and software configurations from unplanned loss.		
Controls		Control Applicability	
		S1	S2
2-7-1	Cybersecurity requirements for backup management must be defined, documented, approved and must include at least the following:	Required	Required
	2-7-1-1 Backups for business-critical systems.	Required	Required
	2-7-1-2 Periodic tests of backup's recovery effectiveness.	Required	Recommended
2-7-2	The cybersecurity requirements for backup and recovery management must be implemented.	Required	Recommended
2-8	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		Control Applicability	
		S1	S2
2-8-1	Cybersecurity requirements for technical vulnerabilities management must be defined, documented, approved and must include at least the following:	Required	Required
	2-8-1-1 Regular patching of systems, software. and devices.	Required	Required
	2-8-1-2 Periodic vulnerabilities scans.	Required	Recommended
	2-8-1-3 Vulnerability remediation, including testing and installation of vulnerability fixes.	Required	Recommended
2-8-2	The cybersecurity requirements for technical vulnerabilities management must be implemented.	Required	Recommended

Public Consultation Version

2-9	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		Control Applicability	
		S1	S2
2-9-1	Cybersecurity requirements for penetration testing exercises must be defined, documented, approved and must include at least 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.	Required	Recommended
2-9-2	The cybersecurity requirements for penetration testing processes must be implemented.	Required	Recommended
2-10	Cybersecurity Event Logs and Monitoring Management		
Objective	To ensure timely collection, analysis and monitoring of cybersecurity events for early detection of potential cyber-attacks or for post-attack analysis.		
Controls		Control Applicability	
		S1	S2
2-10-1	Cybersecurity requirements for event logs and monitoring management must be defined, documented, approved and must include at least the following:	Required	Recommended
	2-10-1-1 Activation of cybersecurity event logs on critical information assets.	Required	Recommended
	2-10-1-2 Subscription with an NCA licensed MSOC service provider.	Required	Recommended
2-10-2	The cybersecurity requirements for event logs and monitoring management must be implemented.	Required	Recommended
2-11	Cybersecurity Incident and Threat Management		

Public Consultation Version

Objective	To ensure the identification, detection, effective management, and handling of cybersecurity incidents.		
Controls		Control Applicability	
		S1	S2
2-11-1	Requirements for cybersecurity incidents management must be defined, documented, approved and must include at least the following:	Required	Required
	2-11-1-1 Response and escalation playbooks to cybersecurity incidents related to data breaches and ransomware attacks.	Recommended	Recommended
	2-11-1-2 Cybersecurity incidents reporting to NCA.	Required	Required
	2-11-1-3 Participation in cybersecurity information sharing with NCA.	Required	Recommended
2-11-2	Requirements for cybersecurity incidents management must be implemented.	Required	Recommended
2-12	Physical Security		
Objective	To ensure the protection of information and technology assets from unauthorized physical access, loss, theft, and damage.		
Controls		Control Applicability	
		S1	S2
2-12-1	Cybersecurity requirements for physical security of information and technology assets must be defined, documented, approved and must include at least the following:	Recommended	Recommended
	2-12-1-1 Secure disposal and re-use of physical assets (including documents and storage media).	Recommended	Recommended
	2-12-1-2 Security of physical access to IT rooms/sensitive electronic devices/mobile endpoints, or documents.	Recommended	Recommended
2-12-2	The cybersecurity requirements for physical protection of information and technology assets must be implemented.	Recommended	Recommended

Public consultation v



Third-Party Cybersecurity

3-1	Third-Party cybersecurity		
Objective	To ensure the protection of assets against the cybersecurity risks related to third-parties including outsourcing and managed services.		
Controls		Control Applicability	
		S1	S2
3-1-1	Cybersecurity requirements for contracts and agreements with third-parties must be identified, documented, approved and must include at least a non-disclosure clause.	Recommended	Recommended

Public Consultation Version

Appendix

Appendix (A): Terms and Definitions

Table 6 below highlights some of the terms and their definitions which were used in this document.

Terminology	Definition
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.

Public Consultation Version

Terminology	Definition
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.
Confidentiality	Maintaining authorized restrictions on access to and disclosure of information, including means of protecting privacy/personal information.
Cryptography	These are the rules that include the principles, methods and means of storing and transmitting data or information in a particular form 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, 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, information technology systems, and operational technologies systems, and their components of hardware and software, services provided, and data they contain from any penetration, disruption, modification unauthorized access, and unlawful exploitation or use. The concept of Cybersecurity includes information security, electronic security, digital security, and the like.
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.

Public consultation version

Terminology	Definition
Event	Something that happens in a specific place (such as network, systems, applications) at a specific time.
Haseen	National Portal for Cybersecurity Services.
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.
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: • 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).

Public Consultation Version

Terminology	Definition
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.
Organization	Private sector organizations, including small, medium, and large companies, and excluding micro-organizations, NGOs, public sector, and CNIs.
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.
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 tiers 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.

Public Consultation Version

Terminology	Definition
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.
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.
Vulnerability	Any type of weakness in a computer system, software, application, set of procedures, or in anything that leaves cybersecurity exposed to a threat.

TABLE 6: TERMS & DEFINITIONS

Public Consultation Version

Appendix (B): List of the Abbreviations

Table 7 below shows some of the abbreviations and their meanings which are used in this document.

Abbreviation	Full Term
CNI	Critical National Infrastructure
DKIM	Domain Keys Identified Mail
DMARC	Domain Message Authentication, Reporting and Conformance
ECC	Essential Cybersecurity Controls
IT	Information Technology
MFA	Multi-Factor Authentication
Monsha'at	Small and Medium Enterprises General Authority
NCA	National Cybersecurity Authority
NCNICC	Non-CNI Private Sector Organizations Cybersecurity Controls
SPF	Sender Policy Framework

TABLE 7: LIST OF ABBREVIATIONS

Public Consultation Version


الهيئة الوطنية
للأمن السيبراني
National Cybersecurity Authority