UNOFFICIAL TRANSLATION

Provided for convenience only. The Arabic original is the sole authoritative text.

Non-CNI Private Sector Entities Cybersecurity Controls

(NCNICC – 1:2025)

National Cybersecurity Authority (NCA)

Sharing indicator: TLP: WHITE | Document classification: Public

Traffic Light Protocol (TLP)

This protocol is used widely worldwide. There are four colours (traffic lights):

Red (personal and confidential, for the recipient only): The recipient may not share material marked red with any individual, whether inside or outside the entity, beyond the defined scope of receipt.

Amber + Strict (sharing within the same entity): The recipient may share the information within the same entity only with the concerned persons.

Amber (limited sharing): The recipient may share the information within the same entity with the concerned persons only, and with those required to take action regarding the information.

Green (sharing within the same community): The recipient may share the information with others in the same entity, or with another related entity or within the same sector; it may not be exchanged or published through public channels.

White / Clear (unlimited).

Executive Summary

Saudi Vision 2030 targeted the comprehensive development of the nation — its security, its economy, and the welfare and dignified living of its citizens. The Vision affirmed the Kingdom's belief in the importance of the private sector, targeting raising its contribution to GDP to 65% by 2030, and raising the contribution of small and medium enterprises to GDP to 35%. Importantly, achieving these outcomes requires strengthening cybersecurity across all private sector entities (small, medium, and large).

Pursuant to Royal Order No. 6801 dated 11/2/1439 AH, the National Cybersecurity Authority is the body competent for cybersecurity in the Kingdom and the national reference for its affairs. Accordingly, the Authority's mandate and competencies address the strategic dimensions and the cybersecurity regulatory dimensions relating to setting policies, governance mechanisms, frameworks, standards, controls, and guidelines, as well as the continuous monitoring of entities' compliance — reinforcing cybersecurity efforts and their importance, and the pressing need that has grown with the increase in threats and security risks in cyberspace, more than ever before.

On this basis, the Authority developed the Non-CNI Private Sector Entities Cybersecurity Controls (NCNICC-1:2025) to achieve a safe and trusted Saudi cyberspace that enables growth

and prosperity. The NCNICC define the cybersecurity controls for small, medium, and large entities in the Kingdom, representing a regulation of the minimum cybersecurity requirements, within three components: Cybersecurity Governance, Cybersecurity Defense, and Third-Party Cybersecurity. This document sets out the details of these controls, their objectives, scope and applicability, and the compliance and monitoring mechanism.

Introduction

The National Cybersecurity Authority (referred to in this document as "the Authority") developed the Non-CNI Private Sector Entities Cybersecurity Controls (NCNICC-1:2025) (referred to in this document as "these Controls") following a comprehensive study of international cybersecurity best practices in small, medium, and large entities. These Controls were developed on the basis of the Essential Cybersecurity Controls (ECC) to provide a version more suitable for entities, within the Controls' scope.

These Controls apply to two categories of entities, per the definition of the General Authority for Small and Medium Enterprises (Monsha'at): the first, large entities; the second, small and medium entities, as specified in Table (1).

Table (1): Categories and number of mandatory NCNICC components

Entity category	Mandatory main components, subcomponents, and main controls
Category (A): Large entities*	3 main components; 22 subcomponents; 65 main controls
Category (B): Small and medium entities*	1 main component; 13 subcomponents; 26 main controls

** Per the definition of the General Authority for Small and Medium Enterprises (Monsha'at).*

Objectives

This document aims to set the minimum cybersecurity controls for Non-CNI private sector entities. The controls are based on leading international cybersecurity practices, enabling such entities to reduce cybersecurity risks arising from internal and external threats. Protecting the entity's information and technology assets requires focus on the core protection objectives, which are:

Confidentiality; Integrity; Availability.

These controls take into account the three core pillars on which cybersecurity rests, which are: People, Process, and Technology.

Scope and Applicability

Scope of the NCNICC

These Controls apply to Non-CNI private sector entities (small, medium, and large) in the Kingdom of Saudi Arabia that are notified by the Authority. All entities outside the scope of these Controls in the Kingdom bear the responsibility of benefiting from them, as appropriate, to implement best practices and strengthen their cybersecurity.

The Controls target two categories: the first (large entities) and the second (small and medium entities). The two categories are based on entity size, in line with the definition of the General Authority for SMEs (Monsha'at). Table (2) shows the entity categories relevant to the NCNICC.

Table (2): Entity categories relevant to the NCNICC

Entity category	Definition	Mandatory components / subcomponents / main controls
Category (A): Large entities*	Entities with more than 250 full-time employees; or achieving more than SAR 200 million in annual revenue.	3 main components; 22 subcomponents; 65 main controls
Category (B): Small and medium entities*	Entities with between 6 and 249 full-time employees; or achieving between SAR 3 million and SAR 200 million in annual revenue.	1 main component; 13 subcomponents; 26 main controls

The Category (A) controls are mandatory for large entities notified by the Authority, while the Category (B) controls are mandatory for small and medium entities notified by the Authority. The Authority may — as it determines — require an entity to comply with additional controls whenever the need arises.

** Per the definition of the General Authority for SMEs (Monsha'at).*

Applicability within the entity

These Controls are designed to suit the cybersecurity needs of Non-CNI private sector entities (small, medium, and large) in the Kingdom, setting the minimum cybersecurity controls for those entities. The applicability of the controls depends on the entity category, within the scope specified in Table (2). The applicability element is illustrated by the following example:

- The sub-controls within main control no. (2-3-1) "Protection of Systems and Information Processing Devices" are applicable and mandatory for both large entities (Category A) and small and medium entities (Category B).
- The controls within subcomponent no. (1-1) "Cybersecurity Management" are applicable and mandatory for large entities (Category A) only.

Implementation and Compliance

In fulfilment of Article Ten, paragraph Three, of the Organizational Arrangement of the National Cybersecurity Authority, all entities within the scope of these Controls must implement what achieves permanent and continuous compliance with them. The Authority — by the mechanism it deems appropriate — assesses entities' compliance with these Controls.

Update and Review

The Authority undertakes the periodic update and review of the NCNICC in accordance with cybersecurity requirements and relevant developments. The Authority also announces and publishes the updated version for implementation and compliance.

Components and Structure of the NCNICC

Main components

The NCNICC comprise three main components: (1) Cybersecurity Governance; (2) Cybersecurity Defense; and (3) Third-Party and Cloud Computing Cybersecurity.

Structure

The framework code is read as NCNICC – 1 : 2025, where NCNICC denotes these Controls, “1” is the version number, and “2025” is the year of issuance.

Each control reference number is composed of four digits — for example 2-3-1-1 — where the first digit is the main component number, the second is the subcomponent number, the third is the main control number, and the fourth is the sub-control number.

Each subcomponent below is presented with its objective, followed by a table of controls. The two right-hand columns indicate the applicability of each control to Category A (large entities) and Category B (small and medium entities), per the legend in Table (5).

Table (5): Control applicability legend

Applicability	Description
Mandatory	The control is mandatory for the entity category, or contains one or more sub-controls that are mandatory for the category.
Recommended	The control is not mandatory for the entity category; however, the entity is encouraged to implement it.

Non-CNI Private Sector Entities Cybersecurity Controls

1 – Cybersecurity Governance

1-1 Cybersecurity Management

Objective: Ensure senior management's support for managing and implementing the entity's cybersecurity programmes.

Ref.	Control	Cat. A	Cat. B
1-1-1	A cybersecurity function must be established within the entity, reporting to the head of the entity or whomever the head delegates. It must be independent of the IT function.	**Mandatory**	Recommended
1-1-2	The headship of the cybersecurity function and the supervisory and sensitive positions within it must be staffed by full-time, highly competent nationals in the cybersecurity field.	**Mandatory**	Recommended
1-1-3	The authorised person must define, document, and approve the entity's cybersecurity governance organizational structure, roles, and responsibilities, and assign the relevant persons; the necessary support must be provided to enforce this, taking into account the avoidance of conflicts of interest.	**Mandatory**	Recommended

1-2 Cybersecurity Policies and Procedures

Objective: Ensure that cybersecurity requirements are documented and disseminated, and that the entity complies with them.

Ref.	Control	Cat. A	Cat. B
1-2-1	Cybersecurity policies must be defined, documented, approved, and disseminated to the relevant personnel in the entity.	**Mandatory**	Recommended
1-2-2	The entity's cybersecurity function must ensure the implementation of the entity's cybersecurity policies.	**Mandatory**	Recommended
1-2-3	The entity's cybersecurity function must review the entity's cybersecurity policies periodically.	**Mandatory**	Recommended

1-3 Cybersecurity Risk Management

Objective: Ensure that cybersecurity risks are managed methodically, with the aim of protecting the entity's information and technology assets.

Ref.	Control	Cat. A	Cat. B
1-3-1	A cybersecurity risk management methodology and procedures must be defined, documented, and approved within the entity.	**Mandatory**	Recommended
1-3-2	The cybersecurity risk management methodology and procedures must be implemented within the entity.	**Mandatory**	Recommended
1-3-3	The cybersecurity risk management methodology and procedures must be reviewed periodically within the entity.	**Mandatory**	Recommended

1-4 Periodic Cybersecurity Review and Audit

Objective: Ensure that the entity's cybersecurity controls are implemented and operating in accordance with the entity's organizational policies and procedures, the national legislative and regulatory requirements issued by the NCA, and the international requirements mandated on the entity.

Ref.	Control	Cat. A	Cat. B
1-4-1	Cybersecurity controls must be reviewed and audited by a party independent of the entity's cybersecurity function, and in accordance with what the Authority approves, in order to assess the entity's compliance with the NCNICC.	**Mandatory**	Recommended
1-4-2	The entity's cybersecurity function must review the implementation of the cybersecurity controls periodically.	**Mandatory**	Recommended

1-5 Cybersecurity Awareness and Training Programme

Objective: Ensure that the entity's personnel have the necessary security awareness and are aware of their cybersecurity responsibilities.

Ref.	Control	Cat. A	Cat. B
1-5-1	Cybersecurity awareness programmes must cover the key topics relevant to cybersecurity that are important for protecting the entity from cyber threats (such as phishing, ransomware, strong passwords, following best practices on social media, and reporting incidents and suspicious behaviour). They must be tailored according to employees' roles and needs.	**Mandatory**	Recommended
1-5-2	The entity's approved cybersecurity awareness programmes must be implemented.	**Mandatory**	Recommended
1-5-3	The entity's approved cybersecurity awareness programmes must be reviewed periodically.	**Mandatory**	Recommended

2 – Cybersecurity Defense

2-1 Asset Management

Objective: Ensure that the entity maintains an accurate and up-to-date asset inventory, including the relevant details for all information and technology assets available to the entity, in order to support the entity's operations and cybersecurity requirements, and to achieve the confidentiality, integrity, accuracy, and availability of the entity's information and technology assets.

Ref.	Control	Cat. A	Cat. B
2-1-1	Cybersecurity requirements for managing the entity's information and technology assets must be defined, documented, and approved.	**Mandatory**	**Mandatory**
2-1-2	Cybersecurity requirements for managing the entity's information and technology assets must be implemented.	**Mandatory**	**Mandatory**
2-1-3	Cybersecurity requirements for managing the entity's information and technology assets must be reviewed periodically.	**Mandatory**	Recommended

2-2 Identity and Access Management

Objective: Ensure the cybersecurity protection of logical access to the entity's information and technology assets, in order to prevent unauthorised access and to restrict access to what is required to accomplish the entity's business.

Ref.	Control	Cat. A	Cat. B
2-2-1	Cybersecurity requirements for identity and access management must be defined, documented, and approved within the entity. They must cover, at a minimum, the following:	**Mandatory**	**Mandatory**
2-2-1-1	*User authentication based on the secure management of username and password.*	**Mandatory**	**Mandatory**
2-2-1-2	*Multi-factor authentication (MFA) for remote access operations, including email and external applications.*	**Mandatory**	**Mandatory**
2-2-1-3	*Management of user authorisations based on the access-control principles of need-to-know and need-to-use, least privilege, and segregation of duties.*	**Mandatory**	**Mandatory**
2-2-1-4	*Privileged access management.*	**Mandatory**	Recommended
2-2-1-5	*Periodic review of identities and access rights.*	**Mandatory**	**Mandatory**
2-2-2	Cybersecurity requirements for identity and access management must be implemented within the entity.	**Mandatory**	**Mandatory**
2-2-3	Cybersecurity requirements for identity and access management must be reviewed periodically within the entity.	**Mandatory**	Recommended

2-3 Protection of Systems and Information Processing Devices

Objective: Ensure the protection of systems and information processing devices — including user devices, servers, and network devices — from cybersecurity risks.

Ref.	Control	Cat. A	Cat. B
2-3-1	Cybersecurity requirements for protecting the entity's systems and information processing devices must be defined, documented, and approved. They must cover, at a minimum, the following:	**Mandatory**	**Mandatory**
2-3-1-1	*Protection from viruses, suspicious software and activities, and malware on servers, user devices, and mobile devices, using modern protection technologies and mechanisms, and managing them securely.*	**Mandatory**	**Mandatory**
2-3-1-2	*Changing default configurations (such as deactivating unnecessary services, changing default passwords, and restricting the use of removable media).*	**Mandatory**	**Mandatory**
2-3-1-3	*Clock synchronisation, centrally and from an accurate and trusted source — such as the source provided by the Saudi Standards, Metrology and Quality Organization.*	**Mandatory**	**Mandatory**
2-3-2	Cybersecurity requirements for protecting the entity's systems and information processing devices must be implemented.	**Mandatory**	**Mandatory**
2-3-3	Cybersecurity requirements for protecting the entity's systems and information processing devices must be reviewed periodically.	**Mandatory**	Recommended

2-4 Email Protection

Objective: Ensure the protection of the entity's email from cybersecurity risks.

Ref.	Control	Cat. A	Cat. B
2-4-1	Cybersecurity requirements for protecting the entity's email must be defined, documented, and approved. They must cover, at a minimum, the following:	**Mandatory**	**Mandatory**
2-4-1-1	*Analysing and filtering email messages, in particular phishing emails and spam emails, using modern email protection technologies and mechanisms.*	**Mandatory**	**Mandatory**
2-4-1-2	*Documenting the entity's email domain through the Haseen platform, using the Sender Policy Framework (SPF), Domain Keys Identified Mail (DKIM), and Domain-based Message Authentication, Reporting and Conformance (DMARC).*	**Mandatory**	**Mandatory**
2-4-1-3	*Protection from Advanced Persistent Threats (APT Protection), which typically use previously unknown viruses and malware (zero-day malware), and managing them securely.*	**Mandatory**	Recommended
2-4-2	Cybersecurity requirements for protecting the entity's email must be implemented.	**Mandatory**	**Mandatory**
2-4-3	Cybersecurity requirements for protecting the entity's email must be reviewed periodically.	**Mandatory**	Recommended

2-5 Network Security Management

Objective: Ensure the protection of the entity's networks from cybersecurity risks.

Ref.	Control	Cat. A	Cat. B
2-5-1	Cybersecurity requirements for managing the security of the entity's networks must be defined, documented, and approved. They must cover, at a minimum, the following:	**Mandatory**	**Mandatory**
2-5-1-1	*Use of network firewalls and secure access gateways.*	**Mandatory**	**Mandatory**
2-5-1-2	*Secure physical or logical isolation and segmentation of network segments.*	**Mandatory**	Recommended

Ref.	Control	Cat. A	Cat. B
2-5-1-3	*Security and protection of wireless networks using secure means for authentication and encryption.*	**Mandatory**	**Mandatory**
2-5-1-4	*Browsing and internet-connection security, including the strict restriction of suspicious websites, file-sharing and storage sites, and remote-access sites.*	**Mandatory**	Recommended
2-5-1-5	*Restriction and management of network ports, protocols, and services.*	**Mandatory**	Recommended
2-5-1-6	*Advanced protection systems for intrusion detection and prevention (Intrusion Prevention Systems).*	**Mandatory**	Recommended
2-5-1-7	*Protection from distributed denial-of-service attacks (DDoS), to reduce the cyber risks resulting from such attacks.*	**Mandatory**	Recommended
2-5-2	Cybersecurity requirements for managing the security of the entity's networks must be implemented.	**Mandatory**	**Mandatory**
2-5-3	Cybersecurity requirements for managing the security of the entity's networks must be reviewed periodically.	**Mandatory**	Recommended

2-6 Mobile Devices Security

Objective: Ensure the protection of the entity's mobile devices (including laptops, smartphones, and smart tablets) from cybersecurity risks, and ensure the secure handling and protection of sensitive information and the entity's business information during transfer and storage where the use of employees' personal devices is permitted (the BYOD principle).

Ref.	Control	Cat. A	Cat. B
2-6-1	Cybersecurity requirements for mobile device security and employees' personal devices (BYOD), where their connection to the entity's network is permitted, must be defined, documented, and approved.	**Mandatory**	**Mandatory**
2-6-2	Cybersecurity requirements for mobile device and BYOD security must be implemented.	**Mandatory**	**Mandatory**
2-6-3	Cybersecurity requirements for mobile device and BYOD security must be reviewed periodically.	**Mandatory**	Recommended

2-7 Data and Information Protection

Objective: Ensure the protection of the confidentiality, integrity, accuracy, and availability of the entity's data and information, in accordance with the entity's organizational policies and procedures and the relevant legislative and regulatory requirements.

Ref.	Control	Cat. A	Cat. B
2-7-1	Cybersecurity requirements for protecting and handling the entity's data and information in accordance with the relevant legislative and regulatory requirements must be defined, documented, and approved. They must cover, at a minimum, the following:	**Mandatory**	**Mandatory**
2-7-1-1	*Use of Data Leakage Prevention techniques and Rights Management techniques.*	**Mandatory**	Recommended
2-7-1-2	*Use of a brand protection service to protect the entity's identity from impersonation (Brand Protection).*	**Mandatory**	Recommended
2-7-1-3	*Security of the use of printers, scanners, and photocopiers.*	**Mandatory**	**Mandatory**

Ref.	Control	Cat. A	Cat. B
2-7-1-4	*Security of asset disposal and reuse (including paper documents and storage media).*	**Mandatory**	**Mandatory**
2-7-2	Cybersecurity requirements for protecting the entity's data and information must be implemented, according to its classification level.	**Mandatory**	**Mandatory**
2-7-3	Cybersecurity requirements for protecting the entity's data and information must be reviewed periodically.	**Mandatory**	Recommended

2-8 Cryptography

Objective: Ensure the proper and effective use of cryptography to protect the entity's technology assets.

Ref.	Control	Cat. A	Cat. B
2-8-1	Cybersecurity requirements for cryptography must be defined, documented, and approved within the entity. They must cover, at a minimum, the following:	**Mandatory**	**Mandatory**
2-8-1-1	*Use of data encryption during storage and transfer.*	**Mandatory**	**Mandatory**
2-8-1-2	*Use of secure and modern encryption methods and algorithms when creating, storing, and transferring data, as well as for all network communication media, in accordance with the requirements of the (basic level) of the National Cryptographic Standards issued by the Authority.*	**Mandatory**	Recommended
2-8-2	Cybersecurity requirements for cryptography must be implemented within the entity.	**Mandatory**	**Mandatory**
2-8-3	Cybersecurity requirements for cryptography must be reviewed periodically within the entity.	**Mandatory**	Recommended

2-9 Backup Management

Objective: Ensure the protection of the entity's data and information and the technical configurations of the entity's systems and applications from unexpected damage resulting from cybersecurity risks.

Ref.	Control	Cat. A	Cat. B
2-9-1	Cybersecurity requirements for backup management must be defined, documented, and approved within the entity. They must cover, at a minimum, the following:	**Mandatory**	**Mandatory**
2-9-1-1	*Performing periodic backups of sensitive business systems.*	**Mandatory**	**Mandatory**
2-9-1-2	*Performing periodic testing to confirm the effectiveness of restoring backups.*	**Mandatory**	**Mandatory**
2-9-2	Cybersecurity requirements for backup management must be implemented within the entity.	**Mandatory**	**Mandatory**
2-9-3	Cybersecurity requirements for backup management must be reviewed periodically.	**Mandatory**	Recommended

2-10 Vulnerability Management

Objective: Ensure the timely detection of technical vulnerabilities and their effective remediation, in order to prevent or reduce the likelihood of such vulnerabilities being exploited in cyberattacks, and to reduce the consequent impact on the entity's business.

Ref.	Control	Cat. A	Cat. B
2-10-1	Cybersecurity requirements for managing the entity's technical vulnerabilities must be defined, documented, and approved. They must cover, at a minimum, the following:	**Mandatory**	**Mandatory**
2-10-1-1	*Updating and patching systems, software, and devices regularly (Patch Management).*	**Mandatory**	**Mandatory**
2-10-1-2	*Periodic vulnerability scanning and detection for all of the entity's assets.*	**Mandatory**	Recommended
2-10-1-3	*Periodic vulnerability scanning and detection for external applications.*	**Mandatory**	**Mandatory**
2-10-1-4	*Managing and remediating vulnerabilities based on their classification, including testing vulnerability fixes before installation.*	**Mandatory**	**Mandatory**
2-10-2	Cybersecurity requirements for managing the entity's technical vulnerabilities must be implemented.	**Mandatory**	**Mandatory**
2-10-3	Cybersecurity requirements for managing the entity's technical vulnerabilities must be reviewed periodically.	**Mandatory**	Recommended

2-11 Penetration Testing

Objective: Test and assess the effectiveness of the entity's cybersecurity defense capabilities, by simulating actual cyberattack techniques and methods, and to discover unknown security weaknesses in the technical infrastructure that could lead to a cyber breach of the entity.

Ref.	Control	Cat. A	Cat. B
2-11-1	Cybersecurity requirements for penetration testing operations must be defined, documented, and approved within the entity. The scope of penetration testing must cover, at a minimum, all externally provided services (via the internet) and their technical components, including: infrastructure, websites, web applications, mobile applications, email, and remote access.	**Mandatory**	Recommended
2-11-2	Cybersecurity requirements for penetration testing operations must be implemented within the entity.	**Mandatory**	Recommended
2-11-3	Cybersecurity requirements for penetration testing operations must be reviewed periodically within the entity.	**Mandatory**	Recommended

2-12 Event Logs Management and Cybersecurity Monitoring

Objective: Ensure the timely collection, analysis, and monitoring of cybersecurity event logs, for the proactive detection of potential cyberattacks or for their analysis after occurrence.

Ref.	Control	Cat. A	Cat. B
2-12-1	Requirements for the entity's event logs management and cybersecurity monitoring must be defined, documented, and approved. They must cover, at a minimum, the following:	**Mandatory**	**Mandatory**
2-12-1-1	*Activating cybersecurity event logs on the entity's sensitive information assets.*	**Mandatory**	**Mandatory**

Ref.	Control	Cat. A	Cat. B
2-12-1-2	*Subscribing to a managed cybersecurity operations centre (SOC) service provider licensed by the Authority.*	**Mandatory**	Recommended
2-12-2	Requirements for the entity's event logs management and cybersecurity monitoring must be implemented.	**Mandatory**	**Mandatory**
2-12-3	Requirements for the entity's event logs management and cybersecurity monitoring must be reviewed periodically.	**Mandatory**	Recommended

2-13 Cybersecurity Incident and Threat Management

Objective: Ensure the timely detection and identification of cybersecurity incidents, and their effective management and handling.

Ref.	Control	Cat. A	Cat. B
2-13-1	Requirements for cybersecurity incident and threat management must be defined, documented, and approved within the entity. They must cover, at a minimum, the following:	**Mandatory**	**Mandatory**
2-13-1-1	*Developing detailed cybersecurity incident response plans (such as for data breaches and ransomware), and the relevant escalation mechanisms.*	**Mandatory**	Recommended
2-13-1-2	*Notifying the Authority upon the occurrence of a cybersecurity incident.*	**Mandatory**	**Mandatory**
2-13-1-3	*Sharing cybersecurity information with the Authority.*	**Mandatory**	**Mandatory**
2-13-2	Requirements for cybersecurity incident and threat management must be implemented within the entity.	**Mandatory**	**Mandatory**
2-13-3	Requirements for cybersecurity incident and threat management must be reviewed periodically within the entity.	**Mandatory**	Recommended

2-14 Physical Security

Objective: Ensure the protection of the entity's information and technology assets from unauthorised physical access, as well as from loss, theft, and sabotage.

Ref.	Control	Cat. A	Cat. B
2-14-1	Cybersecurity requirements for the physical security of the entity's information and technology assets must be defined, documented, and approved. They must cover, at a minimum, the following:	**Mandatory**	**Mandatory**
2-14-1-1	*Protecting physical access to IT rooms and sensitive electronic devices.*	**Mandatory**	**Mandatory**
2-14-1-2	*Protecting physical access to the entity's information and technology assets (such as computers, storage media, and printers) and documents.*	**Mandatory**	Recommended
2-14-1-3	*Protecting surveillance system (CCTV) records.*	**Mandatory**	**Mandatory**
2-14-2	Cybersecurity requirements for the physical security of the entity's information and technology assets must be implemented.	**Mandatory**	**Mandatory**
2-14-3	Cybersecurity requirements for the physical security of the entity's information and technology assets must be reviewed periodically.	**Mandatory**	Recommended

2-15 Web Application Security

Objective: Ensure the protection of the entity's external web applications from cyber risks.

Ref.	Control	Cat. A	Cat. B
2-15-1	Cybersecurity requirements for protecting the entity's external web applications from cyber risks must be defined, documented, and approved. They must cover, at a minimum, the following:	**Mandatory**	Recommended
2-15-1-1	*Use of a Web Application Firewall.*	**Mandatory**	Recommended
2-15-1-2	*Use of the multi-tier architecture principle.*	**Mandatory**	Recommended
2-15-1-3	*Use of secure protocols (such as HTTPS).*	**Mandatory**	Recommended
2-15-1-4	*Clarifying the secure-usage policy for the user.*	**Mandatory**	Recommended
2-15-1-5	*Identity verification, whereby the appropriate verification elements and their number, as well as the appropriate verification techniques, are determined based on the results of assessing the potential impact of failure and bypass of the verification process, for user login operations.*	**Mandatory**	Recommended
2-15-2	Cybersecurity requirements for protecting the entity's external web applications must be implemented.	**Mandatory**	Recommended
2-15-3	Cybersecurity requirements for protecting the entity's external web applications must be reviewed periodically.	**Mandatory**	Recommended

3 – Third-Party and Cloud Computing Cybersecurity

3-1 Third-Party Cybersecurity

Objective: Ensure the protection of the entity's assets from cybersecurity risks related to third parties, including IT outsourcing services and managed services.

Ref.	Control	Cat. A	Cat. B
3-1-1	Cybersecurity requirements within contracts and agreements with the entity's third parties (such as a Service Level Agreement, SLA) must be defined, documented, and approved. They must contain, at a minimum, the following:	**Mandatory**	Recommended
3-1-1-1	*A requirement to maintain the confidentiality of information.*	**Mandatory**	Recommended
3-1-1-2	*Communication procedures in the event of a cybersecurity incident, with the third parties whose handling of the entity's data or the services provided to it may be affected.*	**Mandatory**	Recommended
3-1-2	Cybersecurity requirements within contracts and agreements with the entity's third parties must be implemented.	**Mandatory**	Recommended
3-1-3	Cybersecurity requirements within contracts and agreements with the entity's third parties must be reviewed periodically.	**Mandatory**	Recommended

3-2 Cloud Computing and Hosting Cybersecurity

Objective: Ensure the appropriate and effective treatment of cyber risks and implementation of cybersecurity requirements for cloud computing and hosting. Ensure the protection of the entity's information and technology assets on cloud computing services that are hosted, processed, or managed by third parties.

Ref.	Control	Cat. A	Cat. B
3-2-1	Cybersecurity requirements for the use of cloud computing and hosting services must be defined, documented, and approved. Compliance with the relevant legislative and regulatory requirements must be ensured; and, in addition to the applicable controls within main components (1) and (2) and subcomponent (3-1) necessary to protect the entity's data or the services provided to it, the cybersecurity requirements for the use of cloud computing and hosting services must cover, at a minimum, the following:	**Mandatory**	Recommended
3-2-1-1	*Classifying data before it is hosted with cloud computing and hosting service providers, and returning it to the entity (in a usable format) at the end of the service.*	**Mandatory**	Recommended
3-2-1-2	*Separating the entity's environment (in particular virtual servers) from the environments belonging to other entities within cloud computing services.*	**Mandatory**	Recommended
3-2-2	Cybersecurity requirements for the entity's cloud computing and hosting services must be implemented.	**Mandatory**	Recommended
3-2-3	Cybersecurity requirements for the entity's cloud computing and hosting services must be reviewed periodically.	**Mandatory**	Recommended

Appendices

Appendix (A): Terms and Definitions

Term	Definition
Asset	Anything tangible or intangible that has value to the entity. There are many types of assets; some are obvious, such as people, machines, facilities, patents, software, and services. The term may also include less obvious items, such as information and attributes (the entity's reputation and public image, or skill and knowledge).
Attack	Any type of malicious activity that attempts to gain illegitimate access to, or to collect, disrupt, deny, damage, or destroy, the resources of information systems or the information itself.
Audit	The independent review and examination of records and activities, to assess the effectiveness of cybersecurity controls and to ensure compliance with policies, operational procedures, and the relevant legislative and regulatory requirements.
Authentication	Verifying the identity of a user, process, or device. This is often a prerequisite for allowing access to resources in a system.
Authorization	The property of determining and confirming a user's rights or privileges to access the entity's resources and information and technology assets, and permitting them in accordance with what was predetermined in the user's rights/privileges.
Availability	Ensuring timely access to, and use of, information, data, systems, and applications.
Backup	The copying of files, devices, data, and procedures, available for use in the event of failures, loss, deletion of the asset, or its going out of service.
Confidentiality	Preserving authorised restrictions on access to, and disclosure of, information, including the means of protecting it.
Cryptography	Also called the science of encryption; the rules comprising the principles, means, and methods of storing or transmitting data or information in a particular form, in order to conceal its semantic content, prevent unauthorised use, or prevent undetected modification, such that unauthorised persons cannot read or process it.
Critical National Infrastructure (CNI)	Those essential elements of infrastructure (i.e., assets, facilities, systems, networks, processes, and the key personnel who operate and process them) whose loss or security breach may lead to: a significant negative impact on the availability, integrity, or delivery of essential services — including services that, if their integrity were compromised, could result in significant loss of property and/or lives and/or injuries — taking into account the economic and/or social effects at the national level; and a significant impact on national security, national defence, or the State's economy or national capabilities.
Cyber-Attack	The deliberate exploitation of computer systems, networks, and entities whose operation depends on information technology and digital communications, with the aim of causing damage.
Cybersecurity Risks	Risks that affect the entity's business (including its vision, mission, administration, image, reputation, or operations), its assets, individuals, other entities, or the State, due to the possibility of unauthorised breach, disruption, modification, access, use, exploitation, disclosure, or destruction of networks, IT systems, operational technology systems, their hardware and software components, the services they provide, and the data they contain.
Cybersecurity	As stated in the Authority's organizational arrangement issued under Royal Order No. 6801 dated 11/2/1439 AH, cybersecurity is the protection of networks, IT systems, and operational technology systems, their hardware and software components, the services they provide, and the data they contain, from any

Term	Definition
	unauthorised breach, disruption, modification, access, use, or exploitation. The concept of cybersecurity includes information security, electronic security, digital security, and the like.
Effectiveness	Refers to the degree to which a planned impact is achieved. Planned activities are effective if those activities are actually carried out, and planned results are effective if those results are actually achieved. Key Performance Indicators (KPIs) may be used to measure and assess the level of effectiveness.
Entity	Small, medium, and large private sector entities that are non-CNI, excluding micro entities, non-governmental entities, the government sector, and critical national infrastructure.
Event	Something that occurs in a specific place (such as a network, systems, applications, etc.) and at a specific time.
Haseen	A comprehensive national cyber platform through which the Authority provides centralised and decentralised cyber services and products at the national level to the beneficiary entities (namely government entities, critical national infrastructure entities, and private entities), consistent with the Authority's mandate and competencies and its national cyber regulatory requirements.
Identification	The means of verifying the identity of a user, process, or device. It is usually a prerequisite for granting the right of access to resources in a system.
Incident	An event that occurred on networks, IT systems, or operational technology systems and their hardware and software components, the services they provide, and the data they contain, whether that event was an unauthorised breach, disruption, modification, access, use, or exploitation.
Integrity	Protection against the unauthorised modification or destruction of information. It includes reliability and ensuring non-repudiation of information.
Least Privilege	A core cybersecurity principle aimed at granting a user only the access privileges they need to perform their official responsibilities.
Malware	A programme that infects systems in a covert (often) manner, to violate the confidentiality, integrity, accuracy, or availability of data, applications, or operating systems.
Multi-Factor Authentication (MFA)	A security system that verifies a user's identity by requiring the use of several independent factors of authentication mechanisms. The verification mechanisms include several factors: knowledge (something only the user knows, such as a password); possession (something only the user has, such as a programme or device that generates random numbers, or a one-time password sent for login — referred to as a One-Time-Password); and inherence (a biometric characteristic or trait pertaining to the user themselves, such as a fingerprint).
Need-to-know and Need-to-use	Restrictions imposed on data that is deemed sensitive, unless a person has a specific need to view the data for a purpose related to official business and duties.
Outsourcing	Obtaining (goods or services) by contracting with a supplier or a service provider.
Patch	Supporting data packages to update, repair, or improve a computer operating system, its applications, or its software. This includes fixing security vulnerabilities and other errors; such packages are usually called fixes or bug fixes and improve usability or performance.
Phishing Emails	An attempt to obtain sensitive information — such as usernames, passwords, or credit-card details — for malicious reasons and intentions (in most cases), by disguising as a trustworthy entity in email messages.
Physical Security	Describes the security measures designed to prevent unauthorised access to the entity's facilities, equipment, and resources, and to protect persons and property from damage or harm (such as espionage, theft, or terrorist attacks). Physical security involves the use of multiple layers of interrelated systems, including

Term	Definition
	CCTV, security guards, security perimeters, locks, access-control systems, and many other technologies.
Policy	A document whose provisions set out a general commitment, direction, or intent, as formally expressed by the entity's authorised person. A cybersecurity policy is a document whose provisions set out senior management's formal commitment to implementing and improving the entity's cybersecurity programme, and includes the entity's objectives regarding the cybersecurity programme, its controls, requirements, and the mechanism for its improvement and development.
Privileged Access Management	The process of managing high-risk privileges on the entity's systems, which often require special handling, in order to reduce the risks that may arise from their misuse.
Procedure	A document containing a detailed description of the steps necessary to perform specific operations or activities in compliance with the relevant standards and policies. Procedures are defined as part of processes.
Process	A set of interrelated or interactive activities that transform inputs into outputs. These activities are influenced by the entity's policies.
Recovery	A procedure or process to restore something interrupted, damaged, stolen, lost, or to bring it under control.
Segregation of Duties	A core cybersecurity principle aimed at reducing errors and fraud during the stages of executing a specific process, by ensuring that more than one person, with different privileges, is required to complete those stages.
Third-Party	Any entity acting as a party to a contractual relationship to provide goods or services (this includes service suppliers and providers).
Threat	Any circumstance or event that could negatively affect networks, IT systems, or operational technology systems and their hardware and software components, the services they provide, and the data they contain, whether that effect is an unauthorised breach, disruption, modification, access, use, or exploitation.
Vulnerability	A weakness in networks, IT systems, or operational technology systems and their hardware and software components, and the services they provide, that could lead to an unauthorised breach, disruption, modification, access, use, or exploitation.

Appendix (B): List of Abbreviations

Abbreviation	Meaning
BYOD	Bring Your Own Device
CCTV	Closed-Circuit Television
CNI	Critical National Infrastructure
DKIM	Domain Keys Identified Mail
DMARC	Domain-based Message Authentication, Reporting and Conformance
ECC	Essential Cybersecurity Controls
KPI	Key Performance Indicator
MFA	Multi-Factor Authentication
NCNICC	Non-CNI Private Sector Entities Cybersecurity Controls
NCS	National Cryptographic Standards
SPF	Sender Policy Framework

Translator’s note

This is an unofficial English translation prepared for working reference. The Arabic text published by the National Cybersecurity Authority on its website (nca.gov.sa) is the only authoritative version, and any discrepancy is resolved in favour of the Arabic.

Technical terms, component names, and abbreviations follow the English given in the source document and the NCA’s established English usage (e.g. “Cybersecurity Defense” for the second component). “Mandatory” and “Recommended” render the source’s applicability markers; “the Authority” denotes the NCA throughout.

This translation reflects NCNICC-1:2025 as first issued. Should the NCA publish an official English version, that text should be used in preference to this one.