Cybersecurity Guidelines for Internet of Things

(CGIoT-1:2024)

TLP: White
Document Classification: Public

Disclaimer: The guidelines in this document have been developed based on IoT cybersecurity best practices, and it is for awareness purposes only. NCA assumes no responsibility or liability for direct or indirect results of any actions taken based on the information contained in this document. In addition, any contradictions found between this document and the laws and regulation, the organization shall be subjected to the related laws and regulation. In order to reduce and mitigate cybersecurity risks related to IoT, NCA strongly recommends each organization – if not obligated by related regulations- to regularly conduct their own assessments to those risks.

In the Name of Allah,
The Most Gracious,
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 Recipients 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 amber 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

List of Figures

List of Tables

Executive Summary

The National Cybersecurity Authority has developed the Cybersecurity Guidelines for Internet of Things (CGIoT-1:2024) that are recommended to be applied in all organizations that utilize IoT technologies across the Kingdom, in order to reduce the cybersecurity risks associated with the widespread adoption of IoT.

These guidelines address four main domains: Cybersecurity Governance, Cybersecurity Defense, Cybersecurity Resilience, and Third-Party & Cloud Computing Cybersecurity.

Cybersecurity Governance domain focuses on ensuring that the organization's strategy, vision, roadmap and goals consider the cybersecurity of IoT, including compliance with relevant laws and regulations. It also highlights how IoT cybersecurity policies and procedures are documented and communicated, as well as setting out the management structures for IoT cybersecurity and the roles and responsibilities of all parties. Moreover, it illustrates a methodological approach to cybersecurity risk management and ensures the inclusion of cybersecurity requirements in the information and technology project management lifecycle. In addition, the domain outlines the IoT cybersecurity aspects that should be considered in relation to human resources and IoT cybersecurity awareness and training.

Cybersecurity Defense domain focuses on ensuring adequate cyber defense mechanism are deployed across the IoT ecosystem to safeguard the information and information assets against cyber-attacks; while Cybersecurity Resilience domain instills and reinforces cybersecurity resiliency within the IoT to minimize the impacts caused by cybersecurity incidents.

Third-Party and Cloud Computing Cybersecurity domain emphasizes the need for effective management of cybersecurity risks associated with third parties supporting IoT operations; including the risks associated with cloud computing services.

Additionally, this document provides a set of recommended cybersecurity principles for IoT manufacturers as outlined in Appendix (A), in order to reduce cybersecurity risks associated with IoT products and services.

Introduction

IoT is defined as sensors and devices ("things") that are connected to the internet and/or other networks, which helps to create value based on exchanged data such as easing jobs functions. IoT technology supports many use cases among which smart homes, smart cities, smart healthcare and smart cars. However, due to the increase adoption of IoT, organizations that utilize this technology could be more exposed to cybersecurity risks and threats.

Therefore; National Cybersecurity Authority (referred to in this document as "NCA") developed the Cybersecurity Guidelines for Internet of Things (CGIoT– 1: 2024) after conducting a comprehensive study of multiple international IoT related cybersecurity guidelines, standards, frameworks, and controls, analyzing current status of national initiatives and regulatory requirements, and analyzing previous IoT cybersecurity incidents and attacks. Cybersecurity Guidelines for Internet of Things (CGIoT– 1: 2024) are generic IoT cybersecurity guidelines, Industrial IoT (IIoT) should comply with NCA Operational Cybersecurity Controls (OTCC-1:2022).

The Cybersecurity Guidelines for Internet of Things consist of the following:

- 4 Main Domains.
- 27 Subdomains.
- 81 Guidelines.

In addition, this document contains (11) cybersecurity principles for IoT manufacturers, outlined in Appendix (A).

Objectives

The main objective of this document is to provide a non-mandatory guidance to include cybersecurity best practices in organizations that use IoT technology. These practices are based on industry leading standards which will help organizations limit the cybersecurity risks that originate from internal and external threats.

With the increasing dependency on interconnected technologies, potential cybersecurity risks are introduced within the IoT ecosystem. To safeguard the interests of the stakeholders within an IoT ecosystem, it is recommended to embed cybersecurity consistently into the governance, development, maintenance and management of IoT.

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

- Strategy
- People
- Processes
- Technology

Scope of Work and Applicability

NCA advise every organization in the Kingdom that uses IoT (referred to in this document as "The Organization") to follow these recommended guidelines and implement the minimum cybersecurity best practices in order to minimize cybersecurity risks resulting from the use of IoT technology. In addition, NCA encourages IoT manufacturers to apply these recommended guidelines and the IoT Cybersecurity Principles for Manufactures (outlined in Appendix A) when developing IoT products and services.

Due to the dynamic nature of the cyber threats; the NCA urges organizations and manufacturers to periodically review and assess cyber risks to determine the need to take additional measures regarding IoT cybersecurity.

CGIoT Domains and Structure

Main domains and subdomains of CGIoT

Figure (1) below shows the main domains and subdomains of Cybersecurity Guidelines for Internet of Things

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

Figure 1: CGIoT Main Domains and Subdomain

Structure

Figure (2) and (3) below show the meaning of guidelines codes:

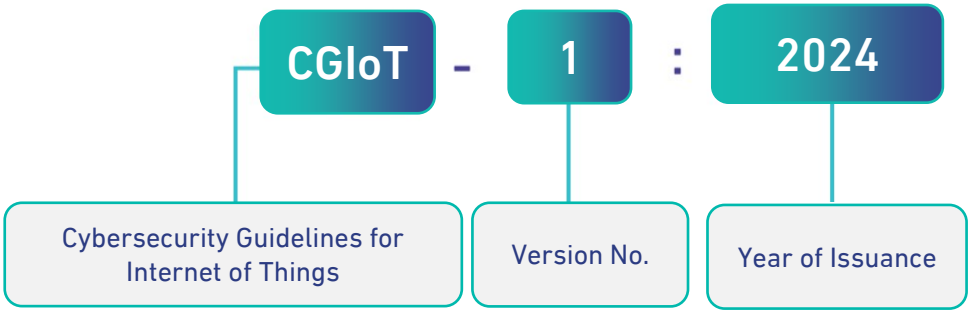

Figure 2: Guidelines Coding Scheme

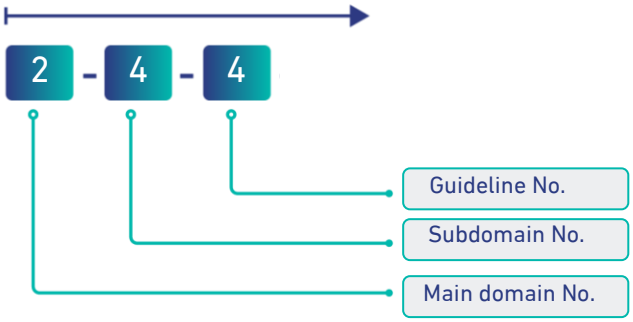

Figure 3: CGIoT Structure

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

1  Reference Number of the Main Domain	Name of the Main Domain
Reference No. of the Subdomain	Name of the Subdomain
Objective	
Guidelines	
Guideline Reference Number	Guideline Clauses

Table 1: CGIoT Structure

Cybersecurity Guidelines for Internet of Things

1 Cybersecurity Governance

1-1	Cybersecurity Strategy
objective	To ensure that an organization's overall cybersecurity strategy, vision, plans, goals, initiatives and projects include IoT cybersecurity aspects, and contribute to compliance with relevant laws and regulations.
Guidelines	
1-1-1	Define, document, and approve IoT cybersecurity requirements within the organization's overall cybersecurity strategy.
1-1-2	Develop, document and implement an IoT cybersecurity plan (within the organizational overall cybersecurity plan) outlining the prioritized actions and initiatives to address the cybersecurity risks identified in relation to IoT within the organization.
1-1-3	Define and track IoT cybersecurity Key Performance Indicators (KPIs) to ensure fulfilment of the cybersecurity requirements throughout the lifecycle of IoT devices.
1-1-4	Periodically review at planned intervals and if necessary, update the strategic initiatives and goals, or upon changes in laws and regulations related to IoT cybersecurity as part of the organization cybersecurity steering committee duties.
1-2	Cybersecurity Policies and Procedures
objective	To ensure that IoT cybersecurity policies and procedures are documented, communicated and complied with by internal stakeholders in the organization, as well as related third parties, as per related laws and regulations, and organizational requirements.
Guidelines	
1-2-1	Define, document, approve and disseminate policies and procedures for the IoT cybersecurity, as part of the organization's overall cybersecurity policies and procedures with the relevant parties inside and outside the organization, including supply chain partners and third-party service providers.
1-2-2	Support policies and procedures by technical security standards including but not limited to (hardening / minimum baseline security standards for embedded systems, authentication and authorization standards, digital certificates, network zoning security standards, etc).
1-2-3	Periodically review at planned intervals and if necessary, update the policies, procedures and standards as per organizational requirements, or upon changes to related laws and regulations.
1-3	Cybersecurity Roles and Responsibilities
objective	To ensure that roles and responsibilities are defined for all the parties, involved in managing, implementing and monitoring IoT cybersecurity requirements within the organization.
Guidelines	

1-3-1	Define, document and approve IoT cybersecurity roles and responsibilities within the organization's cybersecurity governance structure and roles and responsibilities so that cybersecurity requirements are being addressed in accordance with the organization's policies and procedures.
1-3-2	Periodically review at planned intervals and if necessary, update the IoT cybersecurity roles and responsibilities as per organizational requirements, or upon changes to related laws and regulations.
1-4	Cybersecurity Risk Management
objective	To ensure IoT cybersecurity risks are managed using a methodological approach in order to protect the organization's IoT assets as per related laws and regulations, and organizational policies and procedures.
Guidelines	
1-4-1	Define, document, approve, and implement IoT cybersecurity risk management practices, and identify, assess, respond and oversight IoT cybersecurity risks, in order to minimize the impact of potential threats and attacks on the IoT environment, as part of the organization's cybersecurity risk management methodologies and programs.
1-4-2	Define a list of common cybersecurity risk scenarios that could potentially impact the IoT devices and services, related ecosystem or the organization.
1-4-3	Define and document IoT cybersecurity risks in the IoT cybersecurity risk register within the organization's overall cybersecurity risk register.
1-4-4	Conduct an IoT cybersecurity risk assessment considering potential IoT threats, potential scenarios for common IoT attacks, and potential for process disruption and associated damage.
1-4-5	Determine the cybersecurity risks that exceed the risk appetite defined for the IoT and identify suitable risk mitigation measures to lower that risk to, or below, the level of the organization risk appetite.
1-4-6	Periodically review at planned intervals and if necessary, update the IoT cybersecurity risk management procedures and practices as per organizational policies and procedures, or upon changes to related laws and regulations, as well as ensuring they're in alignment with the IoT cybersecurity requirements of the organization.
1-5	Cybersecurity in Information and Technology Project Management
objective	To ensure that IoT cybersecurity requirements are included in project management methodology and procedures in order to protect the confidentiality, integrity and availability of the IoT assets and its components as per organization policies and procedures, and related laws and regulations.
Guidelines	
1-5-1	Implement leading practices related to 'Secure-by-Design' principles throughout the development lifecycle phases of IoT devices and services.
1-5-2	Review the IoT devices and services to ensure that cybersecurity requirements are taken into consideration during planning & design phases of the information and technology projects.
1-5-3	Define a change management procedure for IoT to ensure control over the IoT cybersecurity posture of the organization, including:

	• Considering change management activities throughout the entire IoT systems, devices and services lifecycle phases, including development and integration phase, maintenance or disposal phase, as well as during updates, patches or functionality changes. • Monitoring and communicating changes to the relevant parties within the organization.
1-6	Compliance with Cybersecurity Standards, Laws and Regulations
objective	To ensure that the organization's IoT cybersecurity programs and initiatives are compliant with related standards, laws and regulations.
Guidelines	
1-6-1	Implement adequate enforcement and compliance mechanisms to ensure that organizational IoT requirements, programs, initiatives and activities are compliant with related IoT cybersecurity laws and regulations.
1-7	Periodical Cybersecurity Review and Audit
objective	To ensure that organizational IoT cybersecurity requirements are implemented and in compliance with the organizational policies and procedures, as well as related national laws and regulations, and any other related regulations.
Guidelines	
1-7-1	Review the implementation of IoT cybersecurity requirements, within the organization, periodically by the cybersecurity function.
1-7-2	Review and audit periodically by independent parties outside the cybersecurity function or by third party as part of the overall review and audit of cybersecurity requirements in the organization to ensure implementation and compliance with IoT cybersecurity requirements, and document the results.
1-7-3	Define and implement a process to record and manage any non-compliance with IoT cybersecurity requirements, in addition to assigning roles and responsibilities to implement recommendations and corrective actions to address the identified non-compliance cases, and ensure that summary results and recommendations are made available to accountable individuals within the organization and the cybersecurity steering committee.
1-8	Cybersecurity in Human Resources
objective	To ensure that IoT cybersecurity risks related to personnel (employees and contractors) in organizations are managed effectively during the employment lifecycle as per organizational policies and procedures, and related laws and regulations.
Guidelines	
1-8-1	Define, document, approve, and implement IoT cybersecurity requirements for personnel in organizations (prior to employment, during employment and after termination/separation). This may include: • Cybersecurity induction and ongoing training requirements for personnel, with a specific focus on IoT cybersecurity requirements.

	• Implementation of and compliance with the IoT cybersecurity requirements.
1-8-2	Periodically review personnel access to IoT devices and services, and update or revoke access permissions immediately upon changing roles or termination/separation.
1-8-3	Periodically review at planned intervals and if necessary, update the IoT cybersecurity requirements for personnel in organizations as per organizational policies and procedures or upon changes to related laws and regulations.
1-9	Cybersecurity Awareness and Training Program
objective	To ensure that personnel have essential IoT cybersecurity awareness, and are provided with specific IoT cybersecurity training, skills and credentials needed to accomplish their cybersecurity responsibilities of protecting the organization's IoT assets.
Guidelines	
1-9-1	Include IoT cybersecurity aspects within the organization's overall cybersecurity awareness and training strategy, including: • Define, document, and approve training strategy for personnel with specific IoT roles and responsibilities. • Train employees on cybersecurity best practices for the secure usage of IoT devices and services. • Embed training programs with information about IoT cybersecurity best practices, roles and responsibilities, policies and standards to ensure a safe work environment.
1-9-2	Promote IoT cybersecurity awareness at all organization levels, considering the following; • Keeping personnel aware at all organization levels of the importance of safeguarding IoT devices, including decision-makers. • Conducting cybersecurity activities to raise IoT cybersecurity awareness among personnel, through courses, IoT cybersecurity simulations activties, cybersecurity best practices brochures via e-mail, round tables, and any other awareness channel. • Assessing the IoT cybersecurity skills of personnel to identify knowledge gaps, and efficiently map training against the required skills for each job. • Ensuring that personnel working with IoT devices and services are updated with the latest developments of in the field of IoT cybersecurity.

Cybersecurity Defense

2-1	Asset Management
objective	To ensure that the organization has an accurate and detailed inventory of IoT assets in order to maintain their confidentiality, integrity and availability, in alignment with the organization's cybersecurity and operational requirements.
Guidelines	
2-1-1	Maintain an inventory of the different types of IoT devices and services related assets used by the organization, including naming, classification, sensitivity, components, hardware and software capabilities, as well as those of third parties, as the capabilities of IoT devices vary with their different types, which may expose the oragnization's IoT environment to various risks.
2-1-2	Review periodically the IoT inventory, and track all changes within the organization.
2-2	Identity and Access Management
objective	To prevent unauthorized access to IoT assets and restrict access to what is that is necessary to accomplish tasks for the organization.
Guidelines	
2-2-1	Manage access identities and permissions to IoT assets and restrict access to IoT data, services and devices to authorized users only, based on access and permission control principles (need-to-know-and-use, least privileges, and segregation of duties). In addition to managing privileged access accounts on IoT devices and services.
2-2-2	Implement strong authentication standard to access IoT devices and services, and follow best practices, including but not limited to: • Prevent the users from using default and hard-coded passwords. • Enforce the users to change their passwords periodically. • Improve the complexity of passwords, such as by defining a minimum key length and usage of a combination of letters (upper/lower cases), numbers and symbols; • Implement controls to prevent the display of user's credentials on login interfaces in applications. • Establish threshold limits for unsuccessful attempts. • Enable secure authentication capabilities, if applicable.
2-2-3	Review periodically the IoT access identities and permissions, based on access and permission control principles.
2-3	Email and Messaging Services Protection
objective	To ensure the implementation of cybersecurity requirements for protecting communicating IoT data over email and other messaging services such as SMS, to protect this data from cybersecurity risks.
Guidelines	

2-3-1	Define, document, and approve cybersecurity requirements for protecting the data transmitted between the IoT devices/services and the organization's email and messaging services and review periodically.
2-3-2	Implement cybersecurity requirements for protecting the data transmitted between the IoT devices/services and the organization's email and messaging services, as part of the organization's email and messaging services protection measures.
2-4	Network Security Management
objective	To develop secure and reliable communication and integration capabilities between different IoT devices operating in a network.
Guidelines	
2-4-1	Define, document, approve, and implement cybersecurity requirements for secure connectivity between the IoT devices/services and the intended usage environment including other devices and technology/cloud infrastructure and review periodically.
2-4-2	Implement measures to secure the data communication between different devices connected in a network, including authentication of the peer device with which an IoT device is trying to communicate.
2-4-3	Encrypt and authenticate data transactions between different IoT devices and services, as well as secure the underlying infrastructure, where applicable.
2-4-4	Implement logical and/or physical segregations between IoT environment and organization’s environment based on the organization’s cybersecurity risk assessment, where applicable.
2-4-5	Deploy security gateways to internet-facing IoT devices and services to secure all communication and connectivity to the internet.
2-4-6	Use secure update servers to ensure that the update file for the IoT device software/ firmware, its configuration, and its applications, is transmitted over a secure connection and ensure adequate authentication and encryption mechanisms are put in place to transmit the updates.
2-5	IoT-Connected Mobile Devices Security
objective	To ensure the implementation of cybersecurity requirements for mobile devices (including but not limited to smartphones and smart tablets devices) that are connected to IoT devices and services, to enhance security and reduce the cyber risks.
Guidelines	

2-5-1	Implement the following measures for IoT-connected mobile devices : ● Implement measures to secure the communication between the IoT device and the mobile devices. ● Restrict the access to IoT-connected mobile devices only to authorized personnel. ● Use secure methods of authentication for accessing the mobile device and IoT device data. ● Implement secure code development practices for mobile applications interacting with the IoT devices. ● Secure erasure of IoT devices stored data when losing the mobile device, or when the device is no longer used.
2-6	Data and Information Protection
objective	To ensure confidentiality, integrity and availability of data processed by IoT devices and services.
Guidelines	
2-6-1	Implement IoT data classification and labeling mechanisms for the IoT devices and services as per related laws and regulations, and organizational requirements.
2-6-2	Implement prevention measures to avoid unauthorized access to and tamper with IoT data at rest or in transit.
2-6-3	Prevent IoT devices from collecting sensitive data that is not needed or cannot be adequately protected.
2-7	Cryptography
objective	To ensure adequate use of cryptographic capabilities to secure data transactions and exchange between IoT devices.
Guidelines	
2-7-1	Define, document, approve, and implement cybersecurity requirements for IoT data following the National Cryptographic Standards (NCS-1:2020) and review periodically.
2-7-2	Encrypt the data, both at rest or in transit, where applicable.
2-8	Backup and Recovery Management
objective	To ensure implementation of backup and recovery capabilities within IoT devices and services, in order to protect the data processed by IoT devices from cyber risks.
Guidelines	
2-8-1	Define, document, approve and implement IoT cybersecurity requirements for backup and recovery management as part of the organization's overall backup and recovery management policies and review periodically.
2-8-2	Maintain a tested and trusted version of the IoT software and data stored locally, to enable safe recovery.
2-8-3	Review periodically the stored backups for the IoT devices and test them.

2-9	Vulnerability Management
objective	To ensure timely detection and remediation of vulnerabilities, so as to prevent the probability of exploiting the vulnerabilities to launch cyberattacks against the organization.
Guidelines	
2-9-1	Continuously identify, monitor, and mitigate cybersecurity vulnerabilities within the IoT devices and services.
2-9-2	Patch all the software/firmeware components within the IoT devices in a timely manner as following: • Implement software patches in a preventative manner, to ensure cybersecurity vulnerabilities are eliminated before they can be exploited. • Ensure that the essential function of the device is maintained during software patching. • Utilize the most recent operating system for development the IoT device, as it would help ensure that known vulnerabilities have been mitigated.
2-10	Penetration Testing
objective	To assess and evaluate the efficiency of the organization's IoT cybersecurity defense capabilities through simulated cyber-attacks, in order to discover unknown weaknesses that may lead to a cyber breach.
Guidelines	
2-10-1	Perform penteration testing activties to achieve early detection of vulnerable IoT software and hardware components. The approach can comprise the following: • Identification and analysis of IoT assets within the penteration testing scope. • Verification and exploitation of known vulnerabilities, as well as identification of unknown vulnerabilities (Zero-Day Vulnerabilities) in the IoT devices and services. • Identification and assessment of insecure configurations at the application, network, data, and/ or at the sensor or device gateway level. • Development and Implementation of appropriate reporting and alarming procedures to help prioritize decisions on where and how to incorporate additional cybersecurity measures.
2-10-2	Carry out red team exercises targeting mission critical IoT devices and services to simulate social engineering, physical intrusion, hacking and other deceptive techniques aimed at gaining unauthorized access to critical information and assets, where applicable.
2-11	Cybersecurity Event Logs and Monitoring Management
objective	To ensure regular collection, monitoring and analysis of IoT cybersecurity event logs and threat cases, in order to enable early detection of a potential cyberattacks across IoT devices and services.
Guidelines	

2-11-1	Ensure that IoT devices to have the ability to record cybersecurity events, and centrally store it to be monitored by the Security Operations Center (SOC) in the organization, if possible. Taking into consideration the following: • Define the scenarios to discover potential IoT cybersecurity incidents. • Record events such as user authentication, management of accounts and access rights, attempts to access sensitive data, and modifications to system resources. • Monitor, review and analyze event logs and threat cases for IoT on a regular basis. If possible, implement automated systems to enable real-time monitoring of logs and threat cases. • Leverage data storage services that store the log data in a remote location, instead of storing locally, so that even if the IoT software and hardware components are compromised the log data would remain secure. Implement authentication mechanisms for accessing the data storage to enable secure retrieval of the log data. • In case an unauthorized change or behavior is observed in the IoT assets, alert the consumer and/ or the administrator while ensuring that the device does not connect to a wider network than is necessary to enable the alerting function. • Analyze potential misuse of access privileges by internal stakeholders; • Examine telemetry data collected by IoT devices and services, such as usage, measurement and log data, for cybersecurity anomalies and identifying unusual circumstances in a timely manner. • Establish a retention period for cybersecurity events data. The retention period should be at least 12 months from the date of recording.
2-11-2	Conduct regular examination of diagnostic information for IoT devices, including details such as temperature data, memory usage data, battery life and process execution data to enable better identification of any potential cybersecurity incident.
2-12	Cybersecurity Incident and Threat Management
objective	To ensure timely identification and remediation of threats and IoT cybersecurity incidents in order to minimize the negative impact on the organization's operations.
Guidelines	
2-12-1	Incorporate an IoT incident and threat management model within the overall cybersecurity incident and threat management activities and programs of the organization.
2-12-2	Establish an IoT cybersecurity incident management plan, comprising incident response and handling procedures in alignment with the organization's overall incident management practices. Which can include the following: • Prepare for incidents by ensuring that systems, networks, and applications are secure. • Detect, analyze and document the incident. • Communicate the incident with the stakeholders including the National Cybersecurity Authority (NCA). • Contain, eradicate and recover from the incident. • Create a follow up report for the incident.

2-12-3	Establish a post incident analysis capability to identify and assess the specific software and hardware elements of the IoT devices that were impacted. This analysis should then be utilized to provide the necessary cybersecurity updates or engage in device recall activity (as per applicability) to implement the necessary cybersecurity updates, such as upgrading old firmware with default passwords.
2-12-4	Define IoT cybersecurity requirements for threat management as part of the overall threat modelling process developed by the organization. Implement the following practices as part of the IoT threat management plan: • Monitor, track and aggregate threat intelligence data derived from the usage of IoT devices and services. • Share information regarding breach indicators and threat intelligence with the National Cybersecurity Authority (NCA). • Periodically review the cybersecurity requirements for threat management.
2-13	Physical Security
objective	To ensure the protection of IoT assets from unauthorized physical access, loss, theft and damage.
Guidelines	
2-13-1	Implement physical detection systems to monitor the critical physical environment related to IoT devices and services, which could include server rooms or other workplace areas dedicated towards managing an organization's network, external communication, or external services such as cloud, internet and surveillance.
2-13-2	Implement hardware tamper protection and detection measures for the IoT devices.
2-14	IoT Application Security
objective	To ensure the security and reliability of software applications running on IoT devices.
Guidelines	
2-14-1	Implement technical cybersecurity measures to secure interfaces of IoT applications, in order to reduce the exposure of data, configuration and management operations and prevent unauthorized access.
2-14-2	Implement measures to whitelist certain applications that can run on the IoT device operating system to help prevent execution of unauthorized malware and applications, including untrusted third-party applications.
2-14-3	Implement secure code development practices for IoT applications and conduct source code review to reduce cybersecurity bugs.
2-14-4	The whitelisted applications should be periodically updated to include new applications, functionalities and software patches.
2-15	IoT Device Lifecycle Management

objective	To ensure secure installation and set-up of IoT devices and presence of device withdrawal and replacement plans.
Guidelines	
2-15-1	Utilize hardware that embeds cybersecurity functions at the component level, to maintain protection and integrity of the device, and it is advised to implement the following requirements to secure IoT hardware components, where applicable: • Deploy a Hardware Root of Trust component, which helps in authenticating hardware, firmware, and software components before loading them. It also helps in establishing trust in the boot environment. • Include only essential physical external ports that are necessary for the IoT device to function and enable only trusted connections to access and function on the physical ports.
2-15-2	Define and implement steps for installing and setting up an IoT device and service. It is recommended that these steps are in alignment with cybersecurity best practices regarding the usability of the device and service such as but not limited to: • Apply secure configuration and hardening options that are applicable to the organization, such as disabling certain features or functionalities that would not be used by the organization. • Implement secure set up and configuration to the IoT device, in order to reduce the exposure to threats; such as ensuring all IoT devices and related applications/services don't contain default or hardcoded passwords, and to be unique and complex. • Implement cybersecurity tests prior to deploying the application in the production environment. • Periodically conduct cybersecurity tests before and after every new software release.
2-15-3	Develop and implement a plan for the withdrawal of the IoT devices and services at the end of their lifecycle. Implement the following practices for establishing an end-of-life strategy for the IoT devices and services: • Develop a replacement plan, and an end-of-life plan for the IoT devices and services that have run out of support and/or no longer support the essential cybersecurity functions. Also include third-party components within the end-of-life plan. • Implement measures to securely dispose the data that was stored or being processed by the IoT devices/ service, as per organizational policies and regulations. • Maintain an audit log to monitor the IoT devices and services disposal process.

3 Cybersecurity Resilience

3-1	Cybersecurity Resilience Aspects of Business Continuity Management (BCM)
objective	To ensure the inclusion of IoT cybersecurity resiliency requirements within the overall business continuity management plan of the organization, in order to enhance the integrity of IoT devices and services during cybersecurity incidents.
Guidelines	
3-1-1	Define, document, approve, and implement cybersecurity resiliency requirements for maintaining the confidentiality, integrity and availability of IoT devices and associated components, as part of the business continuity management plan of the organization, and review them periodically. As well as implementing the following: ● Develop resiliency requirements in consideration of how the disruption of an IoT device's essential functions, due to a cyberattack, could impact the business operations associated with it. ● Implement necessary resilience measures that are proportionate to the intended usage of the device, while considering other components that are associated with the IoT system, service or device. ● Ensure essential cybersecurity functions of IoT devices and services are capable of functioning locally in case of a network or power outage and can return to a desired state after the outage.
3-1-2	IoT Endpoint devices, especially gateway devices, shall be capable of enforcing cybersecurity over communication networks and protocols even in the case of a connectivity outage/ disruption to the back-end network, where applicable.

4 Third-Party and Cloud Computing Cybersecurity

4-1	Third-Party Cybersecurity
objective	To ensure the protection of the organizational assets against cybersecurity risks in the IoT devices, procured or operated by a third-party.
Guidelines	
4-1-1	Define, document, approve, and implement IoT cybersecurity requirements within contracts with supply chain partners and third-parties.
4-1-2	Request manufacturers and service providers of IoT products and services to demonstrate the cybersecurity capabilities within their products and/or services, and implement 'Secure-by-Design' principles throughout the development lifecycle phases of IoT devices and services.
4-1-3	Request developers and manufacturers to provide a list of hardware and software components present in the IoT devices and services, to assist in better understanding and managing risk and patching any known vulnerabilities.
4-1-4	Identify IoT information systems, components, and services provided by supply chain partners and third-parties, for inclusion in the overall risk assessment and risk mitigation procedures.
4-1-5	Implement verification activities, through audits, testing and software certifications assurance, to ensure that all IoT third-party components meet the cybersecurity policies of the organizations and the requirements highlighted in their contract.
4-1-6	Review periodically IoT risk mitigation procedures and cybersecurity requirements, that are related to supply chain partners and third-party, to detect any unauthorized procedures.
4-2	Cloud Computing and Hosting Cybersecurity
objective	To ensure implementation of cybersecurity requirements for cloud services that are used for IoT devices.
Guidelines	
4-2-1	Define, document, approve, and implement cybersecurity requirements for cloud services hosting IoT services, as well as other cloud services that are specifically used for IoT devices, in addition to including applicable Cloud Cybersecurity Controls (CCC) and periodically review them.
4-2-2	Implement adequate authorization, authentication, verification and encryption policies and techniques to secure the IoT devices that interact with the private/ self-hosted IoT cloud service and/ or other cloud service specifically being used for IoT devices.
4-2-3	Assess the cybersecurity posture of the cloud service provider and/ or managed service provider to ensure that their cybersecurity posture is in alignment with the organization's IoT cybersecurity policies and procedures.

4-2-4	Establish procedures to facilitate cybersecurity audits, cybersecurity monitoring of IoT-specific data manipulation activities, and management of potential risks associated with existence of a multi-tenant environment in the cloud, as part of the organization's cloud computing and hosting cybersecurity requirements.
4-2-5	Embed provisions in the contractual agreements with cloud service providers and/ or managed service to obtain data stored on cloud platforms in a vendor-neutral format in case of (a planned or unplanned) exit of the cloud service provider and/ or managed service provider from the cloud services agreement.

Appendices

Appendix (A): IoT Cybersecurity Principles for Manufactures

Table (2) bellow illustrates a set of IoT cybersecurity guiding principles that IoT manufacturing companies are encouraged to follow when developing IoT products and services.

No.	IoT Cybersecurity Guiding Principles for Manufactures
1	**Apply** 'Secure-by-Design' and 'Secure-by- Default' principles throughout the development lifecycle phases of IoT devices and services.
2	**Conduct** security testing to verify whether the basic cybersecurity function of the IoT device performs as expected.
3	**Only enable** software services and communication protocols that are required for the intended use or functioning of the device.
4	**Design** embedded systems with Memory Management Units (MMU) and Memory Protection Units (MPU), as microcontrollers alone are unable to provide memory protection capabilities. This should be considered for deployment especially if the organization expects to run untrusted third-party applications.
5	**Implement** mechanisms to ensure all IoT devices and associated applications/ services do not have a default or hard-coded password.
6	**Provide** IoT products consumers with a list of IoT software and hardware components, including those of third-party dependencies.
7	**Conduct** cybersecurity risk assessment for critical IoT devices supply chain.
8	**Ensure** the capability to fail safely and securely is considered when developing critical IoT devices.
9	**Build** secure authentication capabilities in IoT devices.
10	**Minimize** the time gap between discovering a vulnerability in IoT product and releasing the needed security patches.
11	**Inform** IoT products consumers in a recognizable and apparent manner that a security update is required with information on the risks mitigated by that update.

Table 2: IoT Cybersecurity Guiding Principles for Manufactures

Appendix (B): Terms and Definitions

Table (3) below highlights some of the terms and their definitions which were used in this document.

Terminology	Definition
Applications Whitelisting	It is the security practice of specifying an index of approved software applications that are permitted to be present and active on the organization's end-users machines and servers. The goal of whitelisting is to protect the organization's end-users machines and servers from potentially harmful applications.
Authentication	Ensure user's identity, process or device, which is often a prerequisite for allowing access to resources in the system.
Authorization	Identification and verification of the rights of the user to access and allow him/her to view the information and technical resources of the organization as defined in the user rights.
Availability	Ensure timely access to information, data, systems and applications
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.
Data-At-Rest	Inactive data stored in permanent storage media, such as: (Databases, archivals, tapes, off-site back up, laptops and Disks)
Data-In-Transit	Data transmitted from one location to another, by any type of network; such as: Internet, private network, etc.
Internet of Things	Sensors and devices ("things") that are connected to the internet and/or other networks, which helps to create value based on exchanged data such as easing jobs functions.
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 used by the user «such as a program or device generating random numbers or SMSs for login records, which are called: One-Time-Password); and • Inherent Characteristics: (a characteristic of the user ONLY, such as fingerprint).
Secure-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.
Source Code Review	A process that is conducted manually/ automatically to identify security-related weaknesses (flaws) in set of commands and instructions written in one of programming languages.
Telemetry Data	The collection of measurements and other data at remote or inaccessible points and their automatic transmission to a centralized system for monitoring and analysis.

Table 3: Terms and Definitions

Appendix (C): List of the Abbreviations

Table (4) below highlights some of the abbreviations and their meanings which were used in this document.

Abbreviations	Full Term
CCC	Cloud Cybersecurity Controls
CGIoT	Cybersecurity Guidelines for Internet of Things
KPI	Key Performance Indicator
MMU	Memory Management Unit
MPU	Memory Protection Unit
NCS	National Cryptographic Standards
SOC	Security Operations Center
TLP	Traffic Light Protocol

Table 4: List of Abbreviations


الهيئة الوطنية
للأمن السيبراني
National Cybersecurity Authority