UNITED ARAB EMIRATES
MINISTRY OF CABINET AFFAIRS
PRIME MINISTER'S OFFICE

الإمارات العربية المتحدة
وزارة شؤون مجلس الوزراء
مكتب رئاسة مجلس الوزراء

CRITICAL INFORMATION INFRASTRUCTURE PROTECTION (CIIP) POLICY

May 2023 Version 1.0

DISCLAIMER

This document is the sole property of UAE Cyber Security Council and is approved by the UAE Cabinet.

The UAE Cyber Security Council reserves the right to amend, add, or delete any section of this Policy.

Neither the whole nor part of this document shall be reproduced without the prior written consent of the UAE Cyber Security Council.

VERSION CONTROL

Version	**0.1**
Date:	21 February 2022
Prepared by:	CSC
Amendment Content:	Initial Draft

Version	**0.2**
Date:	08 March 2022
Prepared by:	CSC
Amendment Content:	Updates as per initial feedback

Version	**1.0**
Date:	30 August 2022
Prepared by:	CSC
Amendment Content:	Updates as per review comments on the draft v0.2 of the document

	Reviewed by	**Approved by**
Designation:	xxxxxxxxx	xxxxxxxxx
Name:	xxxxxxxxx	xxxxxxxxx
Signature:	xxxxxxxxx	xxxxxxxxx
Date:	xxxxxxxxx	xxxxxxxxx

Table of Contents

Table of Contents

2. CIIP Policies

3. Appendices

SECTION 1

INTRODUCTION

INTRODUCTION

Critical Information Infrastructure Protection (CIIP) is a complex but important topic for nations. Nations at large depend on Critical Infrastructure (CI)[1]services such as energy supply, telecommunications, financial systems, drinking water, and governmental services. CI rely on information infrastructures comprising of operational technologies, information and communication technologies (ICT)-based services and connected technologies, for their functioning. Disruption of these information infrastructures can jeopardize national security and stability, economic growth, citizen prosperity, and daily life, and may have far-reaching impact due to its inherent interconnectedness. The increased digitization in recent years has also opened the door for sophisticated and widespread cyber-attacks, ranging from malware, hackers, hacktivists, and adverse state operations, as a means for attacking critical national infrastructure. The need for effective CIIP strategies, policies and activities therefore becomes increasingly mandatory in most nations.

The Council has established this policy to ensure a baseline measure of security and cyber resilience of its Critical Information Infrastructure (CII), aligned with the UAE's national priority to be a global leader in cyber security; and to implement measures towards a resilient and secure cyberspace for its critical information infrastructure.

1.1 Purpose

This policy aims to strengthen the UAE's cybersecurity posture by defining a consistent and iterative approach to identifying, assessing, and building the national risk profile across its critical information infrastructure.

The policy will further outline the governance mechanism and the protection program for its CII entities, including the identification of CIIs, baseline requirements for the identified entities and the mechanisms for the oversight and enforcement of requirements related to CII protection.

1.2 Scope & Applicability

Critical Information Infrastructure (CII)
Is defined as “interconnected information systems and digital assets, networks, services, and installations which are used to deliver and support the critical national services in the UAE.”

Critical national services are “those physical or virtual services, so vital to the UAE that the incapacity or destruction of such services would have a debilitating impact on national security, economic stability, public health or safety, efficient functioning of the government, or a combination of the above.”

The critical information infrastructure entities include public and private owners and operators, and other entities with a role in securing the UAE’s critical services and include all categories of technology, including Information Technology (IT), Industrial Control Systems (ICS), Cyber-Physical Systems (CPS), and interconnected devices more generally, including the Internet of Things (IoT) and Industrial Internet of Things (IIoT).

The UAE has identified the following sectors as “Critical” considering impact to national security, economic security, public health and well-being, political stability, and relative interdependencies.

This policy is applicable to the CII entities, and relative sector regulators/ designates, and relevant participating stakeholders in the following sectors and sub-sectors, as well as any other sector determined by the CSC.

1.2 Scope & Applicability

Critical Sector	Subsector	Group Name (As per NCSGF)	Type of entity
Energy	Oil	Group A	• Authorities • Operators of Crude Oil exploration, production, refining and treatment facilities, storage, and pipelines • Supply chain and logistics facilities • Central oil stockholding and trading entities • Infrastructure
	Gas	Group A	• Authorities • Operators of Liquefied natural gas (LNG) exploration, production, refining and treatment facilities, storage and pipelines • Supply chain and logistics facilities • Infrastructure
	Nuclear	Group A	• Authorities • Operators of Nuclear power plant enrichment, and spent fuel facilities • Supply chain and logistics facilities • Infrastructure
Transport	Air	Group A	• Authorities • Air carriers • Air Transport authorities • Air Traffic Management • Airport operations companies • Traffic management control operators providing Air Traffic Control (ATC)
	Rail	Group B	• Authorities • Operators • Railway undertaking including operators of service facilities • Infrastructure
	Maritime	Group B	• Authorities • Vessels Operators • Port Authorities and Operators • Managing bodies of ports and entities operating works and equipment contained within ports • Operators of vessel traffic services • Infrastructure
	Road	Group B	• Authorities • Traffic management control • Operators of intelligent transport systems • Infrastructure

1.2 Scope & Applicability

Critical Sector	Subsector	Group Name (As per NCSGF)	Type of entity
Financial	Financial Regulators and Authorities	Group A	• Entities regulated by CBUAE • Credit institutions • Insurance
	Financial Services Providers	Group A	• Payment gateway service provider • ATM service providers
Health	Regulators and Healthcare Authorities	Group B	• Healthcare providers • Healthcare data services • Manufactures/Distributors of medical devices • Manufactures/Distributors of Pharmaceuticals • Research and development laboratories
Electricity & Water	Electricity	Group B	• Electricity undertakings which carry out the function of 'supply' • Generation facility operators • Transmission system operators • Distribution system operators • Nominated electricity market operators • Electricity market participants • District cooling on the promotion of the use of energy from renewal sources
	Infra-structure Water	Group B	• Pipeline and distribution for industries and human consumption • Pumping stations • Desalination plants • Treatment plants
	Authorities and Provider	Group B	• Electricity and water distribution companies and authorities
	Wastewater	Group B	• Sewage treatment plants • Industrial wastewater processing facilities • Sewage pipeline networks

1.2 Scope & Applicability

Critical Sector	Subsector	Group Name (As per NCSGF)	Type of entity
Digital Infrastructure		Group A	• Telecom/Internet Service Providers • DNS Infrastructure providers • Cloud Service Providers • Data Centre Service Providers • Manufactures/Distributors of ICT/ICS/IoT equipment • Internet Exchange Point providers • Submarine Cable Systems • Providers of electronic communications services where their services are publicly available
Government Services	Ministries and Federal Authorities	Group A	• All Federal authorities and Ministries
	Emirates Government level	Group B	• All local government entities within each Emirate
Education		Group A	• Public and Private Entities • Digital services providers for Online Education
Space		Group A	• All relevant entities
Food		Group A	• Food production, processing, and distribution

1.2 Scope & Applicability

Group A

The entities belonging to this group are from the below sectors which predominantly operate within a sector context in the UAE:

- Digital Infrastructure
- Financial Services
- Transport- Air
- Energy- Nuclear
- Energy- Oil & Gas
- Space
- Food
- Education

The entities within the sectors are further classified as CII and non-CII by the identified lead entity for cyber security for the sector.

The entities are expected to align with UAE laws and regulations, adopt a risk-based approach to identify and implement cyber security requirements in line with the National policies, standards, and guidelines including any Emirate and sector specific requirements, and report compliance periodically as applicable.

Group B

The entities belonging to this group are from the below sectors which predominantly operate within each Emirate:

- Transport- Rail, Road & Maritime
- Electricity & Water
- Healthcare

The entities within the sectors are further classified as CII and non-CII by the identified lead entity for cyber security for the sector.

The entities are expected to align with UAE laws and regulations, adopt a risk-based approach to identify and implement cyber security requirements in line with the National policies, standards, and guidelines including any Emirate and sector specific requirements, and report compliance periodically as applicable.

1.3 Adoption Lifecycle

The National Cyber Security Governance Framework (NCSGF) outlines a common integrated approach for managing and adopting cyber security at the entity, sector, and national level. The NCSGF introduces a lifecycle for Understanding, Assessing, Implementing, Monitoring and Collaborating across cyber security within UAE. This lifecycle ensures continual improvement of the UAE’s cyber security capabilities ensuring requirements for securing and protecting Critical Information Infrastructure.

Understanding the complexity, the increasing dependency, applicable laws and regulations, the drivers for prioritization of critical services, changing threat landscape, the challenges of implementing a unified approach for protection of CII.

Assessing the risk on critical services, processes, and digital assets, determining relative impact, assessing current state of security controls implemented, identifying risks of potential breach or failure, and developing plans to mitigate the risks.

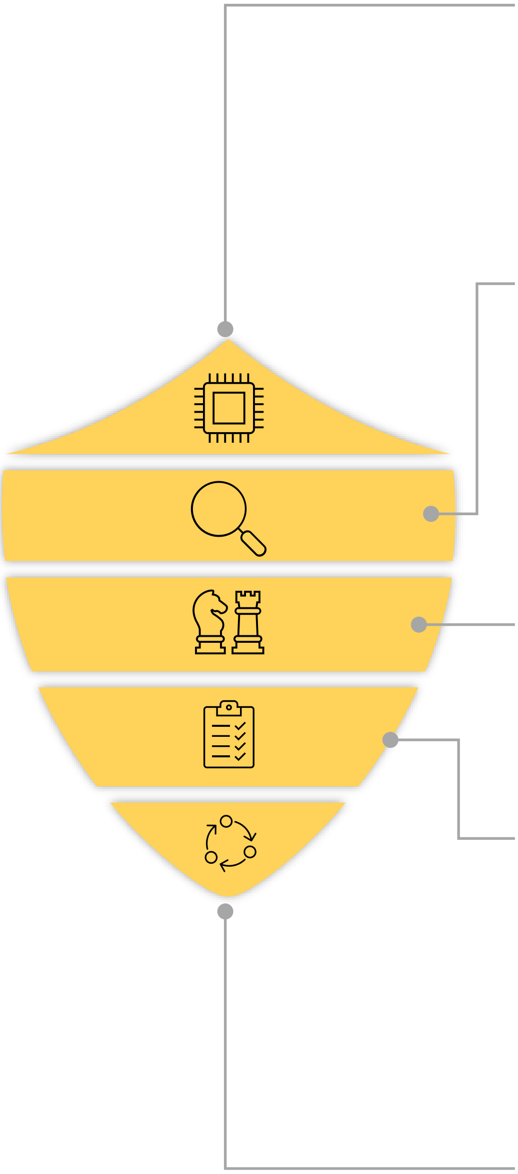
Implementing the identified security controls and best practices adopted within the Nation across critical sectors through continuous collaboration and information sharing.

Monitoring and reviewing the performance and effectiveness of the implemented controls for continual improvement.

Collaborating with other critical sectors, national entities and regional or international industry peers, public and private entities, to share information and adopt best practices.

1.4 Critical Information Infrastructure Protection (CIIP) Principles

The following CIIP principles are laid out as foundational elements for critical information infrastructure protection in the UAE and have been used to develop CIIP policy.



Build national cyber resilience

Reliability, redundancy, response and recovery capabilities are built and maintained across CII entities to drive national cyber resilience.

Sector focused governance

Governance structures are established at each sector to build sectoral capabilities for sectoral needs; enable **focused** interventions and, promote innovation and internal competitiveness in identified sectors.

Risk- based prioritization

Risk based prioritization approach is adopted to identify security measures and build the national critical information infrastructure program.

Establish best practices and standards

Global best practice frameworks are leveraged to provide security assurance and drive compliance efficiencies, while minimum requirements are mandatory for CIIs which are continuously monitored.

Encourage cooperation and partnerships

Effective CIIP needs communication, coordination, and cooperation among all stakeholders on a national and international level to establish a culture of trust and increase national security.

1.5 Exception Approval

A policy exception may be granted by the Cyber Security Council under special circumstances.

Exceptions will be reviewed on a case-by-case basis and their approval is not guaranteed.

SECTION 2

CIIP POLICIES

The following section outlines the policy domains and sub-domains for critical information infrastructure protection. The policy sub-domains further elaborate on the objectives and policy statements

2.1 Governance for CIIP Program

2.1.1 National Level Governance

Version	1.0

Adoption Lifecycle

Understanding	Assessing	Implementing	Monitoring	Collaborating

Policy Objective

To provide oversight and guidance to identified CII sectors, sub sectors, entities, and operators.

Policy Statements

2.1.1.1 The Cyber Security Council shall drive implementation of the CIIP program across all CII sectors, sub-sectors, CII entities and CII operators and to establish a continuous monitoring and reporting regime in alignment with the Ministries, Federal Authorities, Designated Sector Leads and Emirate Leads.

2.1.1.2 The high-level roles and responsibilities of the Designated Sector Leads and Emirate Leads shall be defined in the National Cybersecurity Governance Framework.

2.1.1.3 The entities within each critical sector shall be governed as per the governance model defined in the National Cyber Security Governance Framework.

2.1 Governance for CIIP Program

2.1.2 Emirate Level Governance

Version 1.0

Adoption Lifecycle

Understanding	Assessing	Implementing	Monitoring	Collaborating

Policy Objective

To provide support to the CII entities within Group A, and to help with monitoring of the implementation of the CIIP program.

Policy Statements

2.1.2.1 The Emirate Lead shall support CII entities within Group A, for implementation of national level policies, standards, and regulations within the Emirate, in addition to any Emirate specific issued policies, standards, regulations and cybersecurity/privacy laws.

2.1.2.2 The Emirate Leads, shall monitor implementation of the CIIP program for CII entities within Group A and report compliance to National level entities, as required.

2.1.2.3 List of CII entities shall be maintained, communicated to Cyber Security Council and other relevant authorities, and shall be reviewed periodically.

2.1 Governance for CIIP Program

2.1.3 Designated Sector Level Governance

Version	1.0

Adoption Lifecycle

Understanding	Assessing	Implementing	Monitoring	Collaborating

Policy Objective

To provide guidance and direction to CII entities and operators within a sector and be accountable for implementation of the CIIP program within the sector.

Policy Statements

2.1.3.1 The designated sector lead shall drive implementation of the CIIP program for all Group A entities, along with continuous monitoring of implementation and regular reporting to relevant national entities.

2.1.3.2 Sector regulators/ designated sector lead shall be nominated as the lead entity for their respective sectors and be accountable for ensuring that the activities are being carried out as per the roles and responsibilities listed out in the National Cybersecurity Governance framework.

2.1.3.3 List of CII entities shall be maintained, communicated to Cyber Security Council and Emirate Leads, other sector leads (if needed) and shall be reviewed periodically.

2.1 Governance for CIIP Program

2.1.4 CII Entity/Operator Level Governance

Version 1.0

Adoption Lifecycle

Understanding	Assessing	Implementing	Monitoring	Collaborating

Policy Objective

To ensure CII entities and operators understand their roles and responsibilities towards building a secure information infrastructure.

Policy Statements

2.1.4.1 All CII entities and operators identified as part of this policy shall set up a dedicated security management function and designate/appoint competent personnel/(s) to manage and drive the implementation of the entity's cybersecurity requirements.

2.1.4.2 The security management function shall be responsible for:

- Carrying out annual risk assessment in line with the requirements outlined in the National Cyber Risk Management Framework (NCRMF) or equivalent international best practices, either on their own or via related service agencies, and submit the assessment results as well as improvement measures to the SSGW in charge of CII security.
- Establishing, improving, and designing cybersecurity protection plans for the entity on a continuous basis.
- Establishing entity level logging and monitoring capabilities, which in turn integrate with the sector and national SOC.
- Ensure isolation of OT/ICS network (wherever applicable)
- Formulating emergency plans, carrying out regular emergency drills, and managing cyber security incidents in line with the National Emergency Crisis and Disaster Management Authority NCEMA requirements
- Conducting regular cybersecurity education, technical training, and skill assessments.
- Keeping oversight of third-party products and services by prioritizing purchase of secure and trustworthy products and services, signing security confidentiality agreements, and conducting regular independent audits, where feasible.
- Co-ordinating with regulatory authority informing them (a) regarding any major changes to the critical information infrastructure, that may affect the entity's designation as a CII operator, (b) reporting mergers, divisions, dissolution, or any other major changes to the entity's organization structure. (c) reporting any major issues/threats to cybersecurity.

2.1 Governance for CIIP Program

2.1.5 Supply Chain Management

Version	1.0

Adoption Lifecycle

Understanding	Assessing	Implementing	Monitoring	Collaborating

Policy Objective

To minimize risks from using third party developed software and to secure the data accessed by third party personnel from unauthorized disclosure or tampering.

Policy Statements

2.1.5.1 All CII entities that rely on third parties (for products or services) shall remain accountable for the protection of any critical service ensuring that relevant security requirements are met regardless of whether the CII entity or a third party delivers the service.

2.1.5.2 All CII entities and operators shall establish a supply chain security strategy that requires following a risk management principles and cyber defense in depth approach.

2.1.5.3 All CII entities and operators must consider:

- Using accredited or certified suppliers.
- Conducting background verifications of key third party personnel.
- Enforcing minimum cybersecurity baselines to be followed by suppliers.
- Restricting supplier programs, access, and permissions.
- Authenticating and monitoring all data transmissions.
- Performing security assessments (including technical security assessments) in line with applicable laws, national policies and Emirate or sector specific requirements.
- Signing security and confidentiality agreements clarifying the suppliers technical support, security, and confidentiality requirements.

2.1 Governance for CIIP Program

2.1.6 Data Security and Privacy requirements

Version	1.0

Adoption Lifecycle

Understanding	Assessing	**Implementing**	Monitoring	Collaborating

Policy Objective

To ensure that data is effectively protected and lawfully used through adopting necessary measures, and remain continually in a secure state.

Policy Statements

2.1.6.1 CII entities and operators shall identify and follow applicable data privacy regulations and laws identified at the national as well as Emirate level.

2.1.6.2 CII entities and operators shall classify and protect data based on its importance to the economic development, national security, public interest, and individuals’ and entities’ legitimate rights and interests.

2.2 Risk Profile Development

2.2.1 Identification and prioritization of Critical Services

Version	1.0

Adoption Lifecycle

Understanding	Assessing	Implementing	Monitoring	Collaborating

Policy Objective

To ensure entities identify critical services following a consistent approach.

Policy Statements

2.2.1.1 CII entities shall follow a structured approach for the identification and prioritization of Critical Services, based on best practice principles defined in the NCRMF, which allows for selection of such services based on quantifiable criteria rather than subjective qualitative criteria.

2.2.1.2 Critical service identification process may consider the following factors, in addition to NCRMF guidelines:

- Sector specific criteria – May include but not limited to market share, services with single point of failure, cross-border connectivity, supply of the services to government, industry, or population.
- Dependency – May include but not limited to dependencies with other CI sectors and their critical services/products, supply chain dependencies, dependencies that may carry forward outages in a cascading way, dependencies during emergency or recovery situations.
- Scope of impact - May include but not limited to local, large area or multiple sectors (partially), nationwide or single sector (full), international or multiple sectors (full); size of population affected and/or density of the population in the affected area.

2.2 Risk Profile Development

2.2.2 Conducting Risk Assessment

Version 1.0

Adoption Lifecycle

Understanding | **Assessing** | Implementing | Monitoring | Collaborating

Policy Objective

To ensure all entities conduct regular risk assessment to identify risks to the critical services and underlying information infrastructure.

Policy Statements

2.2.2.1 Entities shall identify the components of each service that are critical to its delivery (i.e., without these components, the delivery of the Critical Service would not occur). It may include but not limited to information systems, digital assets, networks, industrial control systems (ICS) and ICS network, supply chain elements and underlying hardware assets, facilities and personnel supporting the Critical Services.

2.2.2.2 Entities shall conduct annual security risk assessment focusing on critical information infrastructure components identified, for protection from failures related to integrity, availability, and confidentiality.

2.2.2.3 Entities shall analyze impact of threats and vulnerability exposure on the critical information infrastructure components to identify the inherent risks. Also identify any existing controls to finally derive residual risks as per the criteria set within NCRMF.

2.2.2.4 Entities shall establish a risk communication and reporting framework to share the results of risk assessments with relevant sector level and Emirate level regulators and authorities.

2.2 Risk Profile Development

2.2.3 Building the Sector and National Risk Profile

Version 1.0

Adoption Lifecycle

Understanding	Assessing	Implementing	Monitoring	Collaborating

Policy Objective

To build sector and national risk profiles and respective improvements plans to enhance protection measures against identified risks.

Policy Statements

2.2.3.1 All entities within a sector shall communicate with the designated Sector leads/Emirate Leads on “Critical” risks identified and support in building a sectoral risk profile and subsequent sector improvement plans.

2.2.3.2 CSC shall then collaborate with designated sector leads and Emirate Leads, to discuss “Critical” risks identified within each sector, common threats, and cross-sector risks to build a national risk profile and subsequent national improvement plans.

2.3 CII Protection Program

2.3.1 Adopting National Directives on Cybersecurity

Version	1.0

Adoption Lifecycle

Understanding	Assessing	**Implementing**	Monitoring	Collaborating

Policy Objective

To implement and adopt the national cybersecurity requirements.

Policy Statements

2.3.1.1 CSC, in collaboration with Sector Leads/Emirate Leads, shall outline the mandatory cybersecurity policies and standards, extending to sectors and specific CII entities. This shall help in developing the sector CIIP Plan.

2.3.1.2 CSC, in collaboration with Sector Lead and Emirate Leads, shall further outline the National CIIP Program Plan, including any sectoral considerations.

2.3.1.3 All identified CII entities shall implement any cybersecurity policies, control standards, baselines, and plans, as required and mandated by the CSC and/or Sector Leads and Emirate Leads.

2.3.1.4 CII entities shall implement cybersecurity requirements, which are directed at the sector/ industry and are technology/ domain-specific, to protect availability, integrity, and confidentiality of its information infrastructure.

2.3 CII Protection Program

2.3.2 Addressing Digital Interdependencies

Version 1.0

Adoption Lifecycle

Understanding	Assessing	Implementing	Monitoring	Ensuring

Policy Objective

To address systemic risks and reduce adverse impact of digital interdependencies and interrelations between various CIIs, improving resilience and performance of risk reduction measures.

Policy Statements

2.3.2.1 The CII entities shall understand and identify the dependencies and interdependencies on other critical sectors/entities through an assessment of upstream, downstream, and internal dependencies to identify the following areas:

- The products or services provided to entity by another external entity that are necessary to support its operations and functions
- Interdependencies during normal mode of operation and during response to crisis
- Cross-border dependencies
- Interdependencies between public- private enterprises

2.3.2.2 Further an assessment of the type of failure (common cause, propagation, and cascade) shall be used to guide mitigation measures.

2.3.2.3 The protection of confidentiality, integrity and availability of CIIs shall also address the integration of Internet of Things (IoT) devices into critical information infrastructure, and, more generally, the convergence of Information Technology (IT) and Operational Technology (OT).

2.3.2.4 The CII entities shall accordingly develop the CIIP plan based on above considerations.

2.3 CII Protection Program

2.3.3 Information sharing and co-operation

Version	1.0

Adoption Lifecycle

Understanding	Assessing	**Implementing**	Monitoring	**Collaborating**

Policy Objective

To promote a culture of trust among CII stakeholders, including for the exchange of sensitive information and outline the approach for international collaboration.

Policy Statements

2.3.3.1 All CII entities shall implement measures required in the Information Sharing Policy, including measures to identify type of information to be shared and provisions for sharing the required information to identified stakeholders.

2.3.3.2 As established in the National Cybersecurity Governance Model (NCGM), CII entities shall proactively exchange risk and vulnerability information with sector regulators/Emirate Lead and within any information sharing groups, establishing a collaborative environment.

2.3.3.3 CSC shall develop capabilities on a national level to identify new threats and vulnerabilities and shall disseminate relevant and timely information to critical sectors and CII entities.

2.3.3.4 CII entities shall establish and communicate cyber threat information which includes indicators of compromise, tactics, techniques, and procedures used to detect, contain or prevent attacks to national threat intelligence centres.

2.3.3.5 CSC shall outline guidelines for disclosures related to CIIP that contains sensitive or proprietary information and requires enhanced guarantee of confidentiality and digital security, to build trusted relationships for effective public-private co-operation.

2.3.3.6 CSC shall engage in international cooperation and collaboration to secure CIIs, including the development and coordination of emergency warning systems; sharing and analysing relevant vulnerabilities, threats, and incidents information; and coordinating for investigations of cyberattacks on such infrastructures, in accordance with domestic law.

2.3 CII Protection Program

2.3.4 Building National Resilience

Version 1.0

Adoption Lifecycle

Understanding	Assessing	Implementing	Monitoring	Collaborating

Policy Objective

To build national preparedness, response, and recovery capabilities for cybersecurity incidents

Policy Statements

2.3.4.1 CII entities shall ensure all reasonable provisions for building capabilities for prevention of CII disruption and continuity of CII services, are identified and implemented, including technical and technological controls, based on the entities risk assessment.

2.3.4.2 CII entities shall implement the National SOC baseline to ensure that all incident impact levels are commonly understood, a minimum standard for security operations centre (SOC) is maintained and the targeted capabilities and maturity for SOC are achieved.

2.3.4.3 CSC shall create and maintain incident management and crisis communication networks and define requirement for all CII entities in the Cyber Incident Response Framework (CIRF).

2.3.4.4 CII entities shall respond to significant cyber incidents in a coordinated manner as prescribed in the Cyber Incident Response Plan (CIRP), to limit the scope and impact of these incidents.

2.3.4.5 CII entities shall follow any shared standards for addressing sectoral digital security incidents.

2.3.4.6 CII entities shall conduct cyber drills cyber drills to test the resilience of their critical systems/ services and participate in nationwide, sectoral and cross-sectoral tests of cyber resilience.

2.4 Assurance for CIIP Program

2.4.1 Enforcement Mechanism

Version 1.0

Adoption Lifecycle

Understanding	Assessing	Implementing	Monitoring	Collaborating

Policy Objective

To outline the enforcement mechanism for the CIIP program mandates.

Policy Statements

2.4.1.1 CSC shall enforce implementation of the mandatory policies and standards, and institute regular critical information infrastructure security inspection and audits to monitor compliance.

2.4.1.2 The schedule for the inspections and audits shall be defined by the CSC of an annual basis, based on the criticality of the CII entities, and shall be endorsed by the national CIIP working group and the National Cybersecurity Steering Committee (NCSC).

2.4.1.3 Any known/ identified non-compliance to policy mandates shall be escalated to the national CIIP working group and the CSC is expected to intervene in matters impacting national cybersecurity with administrative penalties including fines, operating license revocation or any other action deemed appropriate.

2.4.1.4 Measures to monitor risks and mitigation actions for CII entities, shall be implemented in line with the National Cybersecurity Risk Management Framework (NCRMF).

2.4.1.5 CSC shall raise awareness to facilitate stakeholders’ understanding of the nature and extent of their CII, and the role and expectation of each stakeholder in protecting the CII and subsequently contribute to raising the national cybersecurity.

2.4 Assurance for CIIP Program

2.4.2 Monitoring

Version	1.0

Adoption Lifecycle

Understanding	Assessing	Implementing	**Monitoring**	Collaborating

Policy Objective

To measure the UAE CIIP program effectiveness, identify potential issues, and promote improvement actions.

Policy Statements

2.4.2.1 The CSC shall implement institutional structures and measures to monitor the implementation and effectiveness of the CIIP program, track progress of CIIP actions and routinely verify that the sectoral cybersecurity requirements are being implemented by CII entities, through the following regime:

- CII self-assessment and reporting of the performance on the entity’s CIIP Plan.
- Reporting on consolidated sectoral CIIP Plans and progress of actions by sector leads/Emirate Leads.
- Building the overall national CIIP Program Plan.
- Audits to verify self-assessment reports by the CSC.
- Testing of the implemented information security measures by the CSC.

2.4.2.2 All CII entities shall periodically update the CSC and the sector regulator/ designated authority on the progress of its CII plan implementation, self-assessments and engage during scheduled and/ or unplanned audits and testing exercises. While CII entities may conduct technical assessments, potentially disruptive and intrusive exercise schedules should be communicated to the CSC pre-emptively.

2.4.2.3 The CSC shall endeavor to refine the CIIP program on a continual basis, based on the reported effectiveness of the CIIP program plan and the evolving threat environment and risk profiles.

2.4 Assurance for CIIP Program

2.4.3 Accreditation

Version	1.0

Adoption Lifecycle

Understanding	Assessing	Implementing	Monitoring	Collaborating

Policy Objective

To enable CII to engage with a trusted ecosystem for cybersecurity services and develop minimum standard requirements in the UAE for digital security.

Policy Statements

2.4.3.1 The CSC shall establish the Accreditation Program to encourage a practice for cybersecurity attestation within UAE. CSC shall share a list of accredited service providers, training providers and audit providers.

2.4.3.2 The CII entities shall undergo attestation, based on the defined risk profile, where ‘High risk’ entities are mandated to adhere to the program while ‘Medium and Low risk’ entities are encouraged to adopt the voluntary track defined in the Accreditation Program.

SECTION 3

APPENDICES

3.1 Reference Documents

UAE Policies and Standards

The following UAE policies and standards were referenced when defining these policy statements.

Authority/Body	Document
Cyber Security Council	National Cybersecurity Governance Framework
Cyber Security Council	National Information Assurance Framework
Cyber Security Council	UAE IA Regulation

3.1 Reference Documents

International Standards

The following table outlines the international sources referenced in this document.

Authority/Body	Document
NIS2	Proposal for A Directive on Measures for High Common Level of Cybersecurity Across the Union
UNDRR	Making Critical Infrastructure Resilient
Global Forum on Cyber Expertise (GFCE) Foundation	The GFCE-MERDIAN Good Practice Guide on Critical Information Infrastructure Protection for governmental policymakers

3.2 Abbreviations

Usage	Description
CII	Critical Information Infrastructure
CIIP	Critical Information Infrastructure Protection
CSC	Cybersecurity Council
IT	Information Technology
ISO	International Organization for Standardization
TLP	Traffic Light Protocol
DNS	Domain Name System
IOT	Internet of Things
OT/ICS	Operational Technology/Industrial Control System
SOC	Security Operation Centre

3.3 Definitions

Term	Definitions
Critical Infrastructure	Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on cybersecurity, national economic security, national public health or safety, or any combination of those matters.
Critical Infrastructure Information	Interconnected information systems and digital assets, networks, services, and installations which are used to deliver and support the critical national services in the UAE.
Critical Infrastructure Information Program	Process to maintain a trouble-free functioning of the country's essential information and communication systems.
Cybersecurity	The process of protecting information by preventing, detecting, and responding to attacks.
Cybersecurity Event	A cybersecurity change that may have an impact on organizational operations (including mission, capabilities, or reputation).
Cybersecurity Incident	A cybersecurity event that has been determined to have an impact on the organization prompting the need for response and recovery.
Detect (function)	Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.
Digital Security Incident	An event that may indicate that an organization's IT or digital systems have been compromised or that measures put in place to protect them have failed.

3.3 Definitions

Term	Definitions
Contain	The action of keeping something harmful under control or within limits.
Prevent	Measures implemented prior to a threat event and reduce and/or avoid the likelihood and potential impact of a successful threat event.
Security Operations Centre (SOC)	A command center facility with professionals having expertise in information security who monitors, analyzes and protects an organization from cyber attacks.
ICS	Industrial control system (ICS) is a collective term used to describe different types of control systems and associated instrumentation, which include the devices, systems, networks, and controls used to operate and/or automate industrial processes.
IoT	The internet of things, or IoT, is a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers (UIDs) and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction.
Emergency drills	An emergency drill is a procedure carried out to practice how a building or organization would respond to an unexpected event.
Supply chain security	Supply chain security is the part of supply chain management that focuses on the risk management of external suppliers, vendors, logistics and transportation.
Accredited or certified supplier	Suppliers who are approved and certified to provide products or services.
Single point of failure	A single point of failure (SPOF) is essentially a flaw in the design, configuration, or implementation of a system, circuit, or component that poses a potential risk because it could lead to a situation in which just one malfunction or fault causes the whole system to stop working.

3.3 Definitions

Term	Definitions
Threat	A threat is a potential for a threat-source to exploit a vulnerability successfully.
Vulnerability	Vulnerability is a weakness with an organization's assets that has the potential to allow a threat to occur with greater frequency, greater impact or both.
Risk	The possibility that the occurrence of an event will adversely affect the achievement of the organization's objectives.
Crisis	A crisis is a state of severe disruption, uncertainty and a threat to operations at a fundamental level.
Sensitive Information	Information based on the classification scheme adopted within UAE that can cause harm, inconvenience, or unfairness to an individual or business if it is exposed.
Proprietary information	Information based on the classification scheme adopted within UAE which is highly sensitive information owned by an institution or individual that must not be disclosed to the public.
Resilience	Resilience is the ability of an organization to quickly adapt to disruptions while maintaining continuous business operations and safeguarding people, assets and overall brand equity.
Digital dependence/ interdependence	A dependency is "the relationship between two products or services in which one product or service is required for the generation of the other product or service". An interdependency is "the mutual dependency of products or services".
Framework	A risk-based approach to reducing cybersecurity risk composed of three parts: The Framework Core, the Framework Profile, and the Framework Implementation Tiers. Also known as the "Cybersecurity Framework."
Framework profile	A representation of the outcomes that a particular system or organization has selected from the Framework Categories and Subcategories.