



CYBER INCIDENT RESPONSE PLAN



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: 11 May 2022
Prepared by: CSC
Amendment Content: Initial Draft Document

Version 0.2

Date: 25 June 2022
Prepared by: CSC
Amendment Content: Updated based on 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:	XXXXXXXXXX	XXXXXXXXXX
Name:	XXXXXXXXXX	XXXXXXXXXX
Signature:	XXXXXXXXXX	XXXXXXXXXX
Date:	XXXXXXXXXX	XXXXXXXXXX

Table of Contents

1. Introduction	04
1.1 Purpose	06
1.2 Scope & Applicability	07
1.3 Linkage to the Cyber Incident Response Framework	08
2. Incident Response Roles and Responsibilities	09
2.1 National Cybersecurity Operations Centre (NSOC)	10
2.2 National Cyber Response Group (NCRG)	14
2.3 Sector SOCs and CII operators	18
3. Cyber Incident Response Plan	19
3.1 Prepare	21
3.2 Protect	26
3.3 Detect	28
3.4 Respond	31
3.5 Recover	36
3.6 Learn and Improve	39
4. Appendices	42
4.1 Cyber Incident Alert Schema	43
4.2 UAE Sample IRPs – Typical attack scenarios and playbooks	45
4.3 List of cyber security-related UAE Policies and Standards	48
4.4 Acronyms	49



SECTION 1
INTRODUCTION

INTRODUCTION

Critical Information Infrastructure (CII) in the United Arab Emirates extends across multiple infrastructure sectors and supports essential government and private sector functions, missions, and innovation. As an aspiring global leader in the use of information and communications technology, the UAE is home to ministries, authorities, institutions, businesses, citizens, and residents that are increasingly vulnerable to cyber incidents. The spectrum of threats is wide and evolving, including natural and manmade, deliberate, and unintentional events that can be cross-jurisdictional (i.e., cross-Emirate), cascading across multiple systems and impacting our government, businesses, citizens, and residents.

As global examples repeatedly demonstrated, cyber incidents can quickly increase in scope and severity, defeat individual response measures and cause harm to critical national services. As threats propagate and preventative and protective measures sometimes fail, an incident can rapidly escalate and become a significant cyber incident. This term is used to describe incidents that require national-level intervention, communication and coordination involving multiple stakeholders to be rapidly and effectively resolved to protect the UAE's cyberspace and ultimately its government, private sector, and citizens.

The Cyber Incident Response Framework (CIRF) and Plan (CIRP) support the implementation of the National Cybersecurity Strategy by establishing a national incident management capability and defining how the UAE will prepare for, protect against, detect, respond to, recover, and continuously learn from significant cyber incidents.



1. Introduction

2. Incident Response Roles and Responsibilities

3. Cyber Incident Response Plan

4. Appendices

1.1 Purpose

The CIRF presents the strategic vision and establishes the national capability that enables the UAE and its government and CII sector entities to respond to significant cyber incidents in a coordinated manner, limiting their scope and impact thus ensuring the stability of the UAE cyberspace and contributing to the security, well-being and global competitiveness of the nation.

The CIRP is the high-level national operational cyber incident management plan of the United Arab Emirates.

Its aim is to provide guidance on activities performed collectively by affected stakeholders of the UAE cyber ecosystem, including those at the entity, sector, and federal levels. The main goal of the CIRP is to operationalize the strategic vision for a national cyber incident management capability as laid out by the CIRF and to make sure its strategic purpose is achieved in enabling the UAE to maintain the stability of its cyberspace and to respond to significant cybersecurity incidents as defined by the Cyber Incident Alert Schema (Appendix 4.1).





1. Introduction

2. Incident Response Roles and Responsibilities

3. Cyber Incident Response Plan

4. Appendices

1.2 Scope & Applicability

The CIRF and the CIRP are applicable to all government and private sector entities identified under the Critical Information Infrastructure Protection (CIIP) Policy of the UAE within its geographic borders, including its territorial waters and economic zones.





1. Introduction

2. Incident Response Roles
and Responsibilities3. Cyber Incident
Response Plan

4. Appendices

1.3 Linkage to the Cyber Incident Response Framework

The CIRF outlines the governance model and the incident management lifecycle to successfully respond to significant cyber incidents. The CIRP adds the operational context and interpretation to the framework by providing details on the roles and responsibilities of the various entities involved in incident response during steady state and during cybersecurity incidents. The Plan further provides details on the incident management lifecycle to provide a coordinated response to significant cyber incidents.



SECTION **2**

INCIDENT RESPONSE ROLES AND RESPONSIBILITIES





1. Introduction

2. Incident Response Roles and Responsibilities

3. Cyber Incident Response Plan

4. Appendices



The CIRF defines two national-level governance bodies to manage incident response – the National Cybersecurity Operations Centre (NSOC) and the National Cyber Response Group (NCRG)– while it also includes sector SOCs and CII operators as integral parts of the CIRF. Each of these stakeholders have discrete responsibilities during steady-state and the cyber incident management lifecycle. These responsibilities are defined further in the CIRP.

2.1 National Cybersecurity Operations Centre (NSOC)

The NSOC operated by CSC serves as the central point of operation (technical) for the national cyber incident management of the UAE. It fulfills this primary mission through:

- 2.1.1.1 Providing cyber situational awareness on the UAE's cyberspace through maintaining a national-level common operational picture by the integration of relevant information from all stakeholders (fusion centre function).
- 2.1.1.2 Coordinating cyber incident response on a technical level (technical crisis manager function).
- 2.1.1.3 Serving as the national liaison centre for cyber incident management within the UAE facilitating cooperation and information sharing with members of the UAE cyber ecosystem and key national partners who have additional cyber incident response responsibilities.
- 2.1.1.4 Provide technical and operational advice and information for the NCRG and other relevant stakeholders to synchronize cyber operations, policies, and procedures for cyber incident response.

1. Introduction

2. Incident Response Roles
and Responsibilities3. Cyber Incident
Response Plan

4. Appendices

2.1 National Cybersecurity Operations Centre (NSOC)

Role during Steady-State

The NSOC during steady-state – Level 4–, in its fusion center capacity, maintains a common operational picture for and provides cyber situational awareness about the UAE’s cyberspace to stakeholders at the entity, sector and national levels. The common operational picture enables CSC to defend UAE cyberspace and coordinate national-level incident response activities, esp. during significant cyber incidents. The NSOC leverages the reporting and information sharing process outlined below and, as per the incident response framework, to build and maintain the common operational picture. To deliver on this core function, the NSOC maintains a national Point of Contact system, dedicated for the purposes of technical cyber incident management serving as the designated channel for reporting and information sharing with sector-specific Computer Emergency Response Teams (CERTs, including national-level aeCERT) and CII entities. Reporting and information sharing rules and requirements are defined below. The NSOC analyzes all available information to deliver the common operation picture on the UAE cyberspace.

The NSOC during steady-state – Level 4–, in its technical crisis manager function, implements activities defined by the Cyber Incident Management Lifecycle, including incident logging, validation, correlation and analysis, coordination and alert, identify containment, mitigation and recovery strategies, alongside providing additional subject matter expertise as required to close the incident. The NSOC may provide technical assistance to CII entities to respond to Level 4 incidents. Technical assistance includes providing cyber situational awareness, guidance on response activities for entities to take and technical response expertise (e.g., threat mitigation and incident resolution) as requested, on a case-by-case basis. To facilitate cooperation, information sharing and incident response, NSOC may send personnel to key stakeholders, including sector SOCs and CII entities on a temporary or permanent basis to maintain trusted relationships, enhance reporting and/or information sharing and coordinate action during the cyber incident response lifecycle. Conversely, sector SOCs and key CII entities might also be invited to send personnel to NSOC to fulfil similar roles.

¹ Detailed definition incident levels is provided in the Framework and in Annex 4.1 - Cyber Incident Alert Schema.

1. Introduction

**2. Incident Response Roles
and Responsibilities**3. Cyber Incident
Response Plan

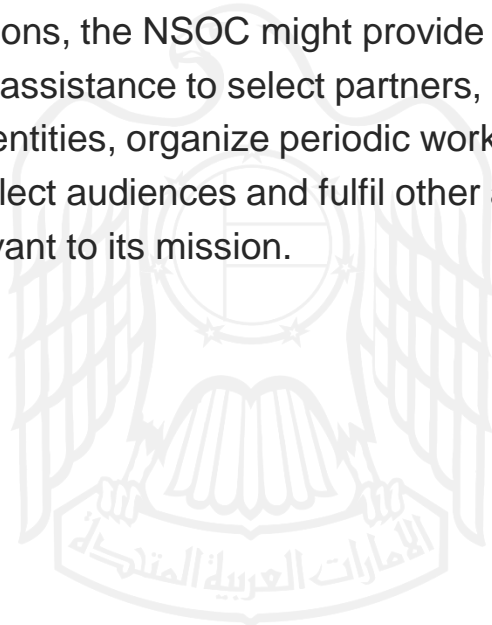
4. Appendices

2.1 National Cybersecurity Operations Centre (NSOC)

Lastly, the NSOC also serves as the national liaison center for cyber incident management within the UAE. Accordingly, it engages with key national partners who have additional or complementary cyber incident response roles and responsibilities to facilitate information sharing to prepare for, protect against, and respond to cyber incidents on all alert levels. The roles and responsibilities required for optimal cooperation are described below (2.5 Other National Partners with Cyber-related Roles and Responsibilities).

To enhance collaboration, NSOC is to maintain a formal Incident Response Working Group that meets monthly to share information on cyber threats, vulnerabilities, response activities and lessons learned. The Working Group will include representatives from sector regulators, aeCERT, sector SOCs and CII entities as well as ICT managers and SOC/CSIRT managers from government and other relevant stakeholders. The Incident Response Working Group will enable the NSOC to build more formal relationships with operations centers to improve coordinated response during Cyber Incidents.

In addition to its above core functions, the NSOC might provide direct support or information assurance assistance to select partners, including designated public administration entities, organize periodic workshops to facilitate knowledge transfer to select audiences and fulfil other awareness raising and training activities relevant to its mission.



1. Introduction

2. Incident Response Roles
and Responsibilities3. Cyber Incident
Response Plan

4. Appendices

2.1 National Cybersecurity Operations Centre (NSOC)

Role during Significant Cyber Incidents (Level 3)

Acting in its fusion centre capacity, NSOC serves as the national focal point for developing cyberspace situational awareness. Consequently, the NSOC is the primary point of contact for entity, sector, and national-level organizations to report relevant cyber incidents as well as share information as defined by the Reporting requirements and Information Sharing chapter. The above serves as the basis of the Common Operational Picture maintained by NSOC. Building on this overarching cyber situational awareness, the NSOC is to:

- Analyze available incident and threat information and recommend to the CSC Chair that a Significant Cyber Incident (Level 3) to be declared and the NCRG be convened when needed; advise the NCRG Chair on the composition of the NCRG based on the nature, scope, and potential or actual impact of the incident²; and act as the technical coordinator of those bodies (notifications, logistics, etc.).
- Advise and inform the NCRG when convened on the real or potential impact of the incident, response and recovery actions, and strategic policy updates.
- Coordinate response activities and provide technical assistance to CII entities and other relevant stakeholders, including critical national services at risk, including incident prioritization, capability allocation, and communicating cyber incident-related situational awareness.
- Engage with international cybersecurity partners when instructed to (e.g., international cybersecurity centers, CERTs, and other organizations) to help overcome an incident; and
- Provide crisis communication to maintain public confidence and provide emergency public communications services under the strategic guidance and supervision of the NCRG and other relevant national authorities if needed.

To ensure NSOC can deliver on its above core responsibilities and fulfill its mandate, the NSOC in collaboration with the Incident Response Working Group is to develop, test, maintain and update a national Incident Management Plan. Following international best practice and industry standards, the Incident Management Plan, a highly detailed, operational incident management document should clearly define, and document required course(s) of action to manage incidents covering all phases of the cyber incident management lifecycle.

² For example, if the incident is primarily associated with the Oil and Gas and Utilities Sectors, representatives from those critical infrastructure sectors will actively participate in NCRG activities while the participation of other critical infrastructure sectors may be limited.'

³ 'Crisis communications activities include informing businesses, citizens, and residents about threats to CII, providing information about the incident, and recommending steps that stakeholders and the public can take to protect themselves and minimize impact from the incident. Effective crisis communications have elements of both speed and accuracy, conveying actionable information, and increasing chances of the public's resilience during and following a Significant Cyber Incident.'

1. Introduction

**2. Incident Response Roles
and Responsibilities**3. Cyber Incident
Response Plan

4. Appendices

2.2 National Cyber Response Group (NCRG)

The NCRG is a strategic decision-making body responsible for coordinating cyber incident management across the UAE in response to declared Significant Cyber Incidents at Level 3.

Specifically, the NCRG:

- 2.2.1.1 Coordinates resources and actions to help system owners who need assistance with handling incident response, including containment and remediation.
- 2.2.1.2 Identifies joint solutions for mitigation, relying on the NSOC for technical advice as defined above; and
- 2.2.1.3 Provides organizational leadership and oversight throughout the entire incident response lifecycle.



1. Introduction

2. Incident Response Roles
and Responsibilities3. Cyber Incident
Response Plan

4. Appendices

2.2 National Cyber Response Group (NCRG)

Membership

The NCRG is comprised of high-level decision-makers of national partners and critical infrastructure sector regulators and entities based on the scope of the incident.

National Cyber Response Group (NCRG) Ecosphere

High-level representatives of critical infrastructure sector regulators, SOCs and operators identified by the Critical Information Infrastructure Protection Policy (CIIP) of the UAE⁴ will also be invited to participate in the NCRG. Representatives of each critical infrastructure sector may vary based on the organization of each sector. If a sector has a regulator, the regulator should serve as one of the sector representatives on the NCRG.

CSC serves as the NCRG Chair and as such approves its composition. NSOC serves as technical coordinator and its Director is also a member of the NCRG.

Representatives serving as Members of the NCRG shall be high-level decision-makers of their organization with relevant expertise and capable of leveraging their respective organization's resources as part of the cyber incident management process on a national level. In addition, critical infrastructure sector representatives are expected to represent their entire sector on the NCRG and consequently be able to provide information on the potential or actual impact of a Significant Cyber Incident on their sector.



1. Introduction

**2. Incident Response Roles
and Responsibilities**3. Cyber Incident
Response Plan

4. Appendices

2.2 National Cyber Response Group (NCRG)

Role during Steady-State

During Steady-State the NCRG is to meet on a quarterly basis to consider the implications of changes to the UAE cyberspace environment, review and evaluate governance processes and manage performance of national incident response capabilities and ensure lessons learned from incidents are addressed.

The NCRG Chair, with input from the NSOC, will evaluate lessons learned from testing, exercises and previous incidents and monitor the implementation of remediation to ensure that lessons learned are acted upon. The NSOC, leveraging its Incident Response Working Group, is to conduct gap analysis and present lessons learned for NCRG consideration. The NCRG will make decisions on then monitor implementation of relevant action plans required to address gaps and lessons learned. NCRG Members will be expected to provide regular status updates regarding how action plans are implemented, and lessons learned are leveraged vis-à-vis their respective sectors.

Regular meetings during Steady-State promote collaboration and coordination among the NCRG Membership and will enhance the NCRG's preparedness to convene and respond rapidly in the event of a Significant Cyber Incident. In addition, the NCRG may participate in national and sector-specific exercises that are designed to test cyber response plans and capabilities and prepare for Significant Cyber Incidents. The NCRG Chair will ensure that the appropriate resources are made available to support all NCRG activities.



2.2 National Cyber Response Group (NCRG)

Role during Significant Cyber Incidents (Level 3)

If relevant thresholds or incident indicators are met defined by the Cyber Incident Alert Schema, based on the recommendation of the NSOC, the NCRG Chair is to declare a Significant Cyber Incident – **(Level 3)**.

If a Level 3 cyber incident is declared, the NCRG Chair is to decide on the NCRG's given composition and convene a meeting (physical, virtual or hybrid), prepare the agenda and initial or scheduled requests for information in response to the incident from relevant NCRG Members. NSOC is to assist by providing technical expertise and coordination. NCRG Members are to provide timely information and engage actively in NCRG activities to aid cyber incident response efforts.

During a Significant Cyber Incident, NCRG Members are responsible for having familiarity with current cyber incidents in their mission area and represent their organization in discussions related to the resolution incidents and commit necessary resources and capabilities. NCRG Members jointly determine objectives and priorities for incident response and agree upon a documented cyber Incident Resolution Plan, then work together to execute it in response to Significant Cyber Incidents. The NCRG will complete its activities when:

- a) The goals outlined in the Incident Resolution Plan have been achieved and the Cyber Incident Alert Level has been returned (de-escalated) to Level 4 or Normal levels; or
- b) The NCRG is to escalate and CSC after consultation with NCEMA shall declare a Cyber Incident Level 2 in case relevant thresholds and incident indicators defined by the Cyber Incident Alert Schema are met.



1. Introduction

**2. Incident Response Roles
and Responsibilities**3. Cyber Incident
Response Plan

4. Appendices

2.3 Sector SOCs and CII operators

Sector SOCs and CII entities are core stakeholders of the UAE cyber ecosystem and accordingly fundamental components of its cyber incident response capability. These stakeholders are to play a key role both during Steady-State and while participating in national response efforts in reaction to Significant Cyber Incidents. The list of identified CII entities are defined in the CII Protection Policy done by CSC.

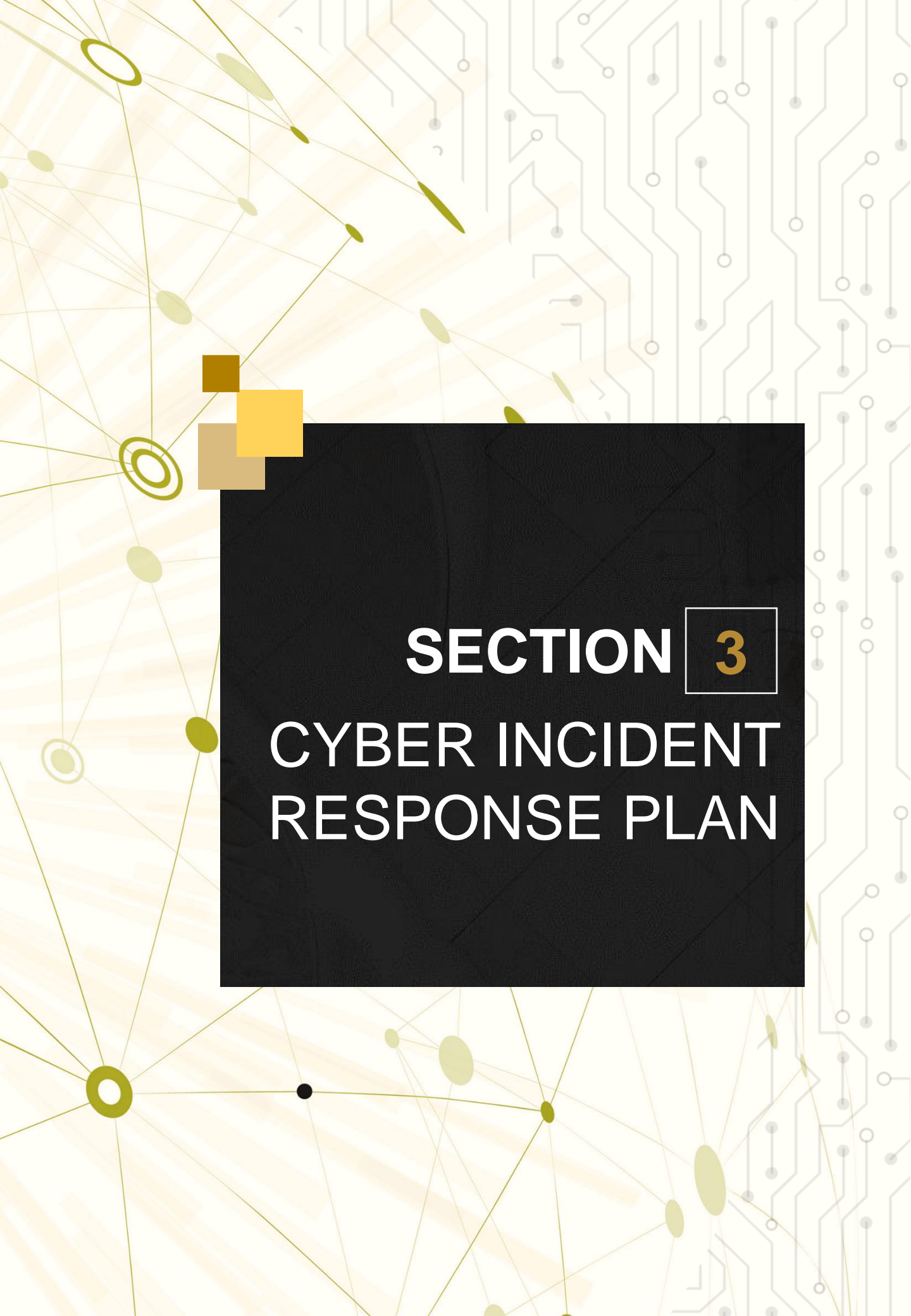
Role during steady state

Sector SOCs and CII entities are to maintain their own baseline incident response capabilities and leverage them independently during Steady-State Normal status and in cooperation with NSOC during Level 4 and 3 Cyber Incident level. These actors are also having the primary responsibility to fulfil their mandatory and (optional) voluntary incident reporting and information sharing responsibilities as defined by the Plan.

Roles during Significant cyber incident

During Significant Cyber Incidents , sector SOCs and CII entities are to cooperate with and leverage their own resources in coordination with NSOC while participating in the cyber incident response effort.

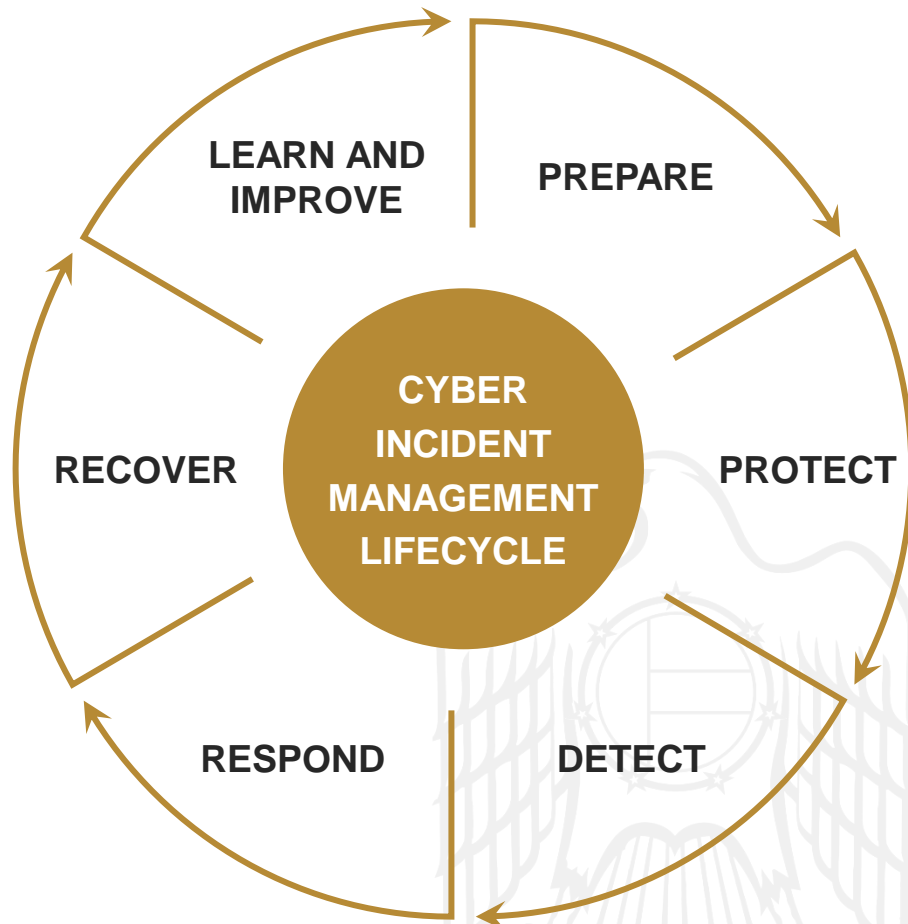




SECTION 3
**CYBER INCIDENT
RESPONSE PLAN**

1. Introduction	2. Incident Response Roles and Responsibilities	3. Cyber Incident Response Plan	4. Appendices
-----------------	-------------------------------------------------	----------------------------------------	---------------

The CIRP guides activities of all CIRF stakeholders through the phases of the cyber incident management lifecycle, including the transition from Steady-State to Significant Cyber Incident and back to Steady-State. The cyber incident management lifecycle defines key roles, tasks, and responsibilities of each actor. Effective execution of the CIRP requires integrating and harmonizing stakeholder incident management plans, policies, and capabilities at the entity, sector, and national levels. Integration will enable faster, more coordinated national-level response to Significant Cyber Incidents.



I. Cyber Incident Management Lifecycle

3.1 Prepare

Due to the dynamic nature of the cyber threat environment, not all incidents can be prevented. Preparedness is thus essential to provide the swiftest incident response and recovery possible. Accordingly, this phase aims to establish the capability (people, processes, and technology) of cyber incident response, including reporting and information sharing enabling cyber situational awareness.

CII Entity

General tasks

- Maintain industry standard CSIRT/SOC (or equivalent) capability to manage cyber incidents.
- Establish relationships with designated operational entities (sector SOCs, aeCERT, NSOC) to meet reporting and information sharing requirements and to establish access to sector-specific and national cyber situational awareness information and technical assistance.
- Conduct and participate in exercises of cyber incident response testing capabilities, policies, plans, and procedures (including exercising large-scale cyber incidents that have physical consequences).

People

- Connect cyber incident response personnel with business continuity and emergency management personnel (functions).
- Invest in professional development of cyber incident response personnel, including training Members on the CIRF and CIRP and any supporting plans, procedures, and technology at the national, sector, or entity levels.
- Conduct end-user cybersecurity awareness training.
- Ensure in the event of possible conflicts of interest, the incident management staff assigned must be sufficiently independent to avoid the appearance of a conflict of interest.

1. Introduction

2. Incident Response Roles
and Responsibilities3. Cyber Incident
Response Plan

4. Appendices

3.1 Prepare

CII Entity

Process

- Maintain asset and risk management functions based on industry best practice.
- Develop and maintain entity-specific cyber incident response plans and standard operating procedures aligned with the CIRF, CIRP and sector-specific plans, as appropriate.
- Carry out regular gap- or maturity assessments and develop a roadmap for remediating identified gaps in cyber incident response capabilities.
- Connect cyber incident response and business continuity management processes.

Technology

- Establish and maintain industry standard technological capabilities (including physical security) required for incident management, including threat intelligence, monitoring, and response activities as well as reporting and sharing (incl. automated).

3.1 Prepare

Sector SOC, aeCERT

General tasks

- The SOC strives to build the local security community, helping raise awareness, and offering education to organizations that need it. It is dedicated to establishing partnerships, providing resources and a feedback mechanism for all organizations within the UAE.
- Specifically, the SOC is to maintain all baseline capabilities and provide services as defined in the SOC Baseline Policy done by CSC.

People- Process

- Establish, build, and maintain incident responder network within their respective sectors and liaise with national organizations (aeCERT, NSOC).
- Assist sector regulator (or equivalent) and NSOC to assess and manage incidents.
- Aggregate information on sector-level preparedness and develop industry standard metrics aligned with reporting and sharing requirements.
- Contribute to the development and maintenance of sector-specific cyber incident management plans and procedures under the tenets of the CIRF and aligned with the CIRP.
- Conduct and participate in sector-level exercises testing cyber incident response capabilities, policies, plans, and procedures (including exercising large-scale cyber incidents that have physical consequences).

Technology

- Develop and maintain tools, equipment, and supporting infrastructure to identify, collect, analyze, produce, and share/publish information necessary to prepare for incidents.

3.1 Prepare

National Security Operations Centre (NSOC)

General tasks

- Establish, build, and maintain relationships with stakeholders at the entity, sector, national, and international levels.
- Develop and maintain a common operational picture providing national-level cyber situational awareness.
- Maintain capability (incl. personnel, processes, and capabilities) to serve as top national-level incident response center providing technical response to affected CII entities and sectors and assisting the NCRG during incidents.
- Maintain capability to assist the NCRG with logistical and administrative tasks.
- Conduct and participate in national/federal-level exercises testing cyber incident response capabilities, policies, plans, and procedures in coordination with the relevant stakeholders (including exercising cyber incidents that have physical consequences).
- Audit or assess sector-level incident response plans and capabilities and provide recommendations for improvement.

People

- Invest in professional development of personnel to keep up to date with emerging technologies and the evolving threat environment.

Process

- Maintain nation-wide process integrating cyber incident response reporting and sharing activities to generate a common operational picture.
- Prepare and maintain processes enabling national cyber incident response.
- Establish processes assisting NCRG and enabling response to significant cyber incidents (coordination, logistics).

Technology

- Maintain industry standard tools, systems and supporting infrastructure to aggregate information and generate common operational picture and deliver on cyber incident management.

1. Introduction

2. Incident Response Roles
and Responsibilities3. Cyber Incident
Response Plan

4. Appendices

3.1 Prepare

National Cyber Response Group (NCRG)

General tasks

- Meet quarterly to review the status of actions to implement lessons learned and evaluate performance of the national cyber incident management capability.

People

- Appoint relevant Member(s) representing relevant entities and provide them with relevant information on the process, the CIRF and the CIRP.

Process

- Establish processes and protocols for convening, meetings, and logistics with the assistance of NSOC and under the leadership of the NCRG Chair.



3.2 Protect

Following strategies to protect CII and thereby decreasing the number of incidents is an important element of incident management. If security controls are insufficient, higher volumes of incidents may overwhelm an incident response capability at the entity or sector level. This can lead to inadequate response, which can translate to a greater impact on critical infrastructure sectors or the UAE. The Protect Phase outlines actions that are necessary to protect decrease the number of incidents and mitigate or decrease their impact.

CII Entity

General tasks

- Maintain industry standard asset management, vulnerability management and hardening processes as well as threat intelligence and baseline SOC capabilities, including monitoring, intrusion prevention and detection.
- Implement penetration testing according to CIIP Policy and internal requirements following industry best practice.
- Maintain coordination with sector regulators and NSOC to gain up-to-date knowledge on policy, national-level network, or technology changes.



1. Introduction

2. Incident Response Roles
and Responsibilities3. Cyber Incident
Response Plan

4. Appendices

3.2 Protect

Sector SOCs, aeCERT

General tasks

- Monitor and track threats, vulnerabilities, disruptions, and intrusions contributing to the maintenance of the common operational picture at a NSOC level. Collect and provide additional information gathering data feeds from continuous monitoring, risk assessment results, infrastructure enhancements and developed indicators and metrics.
- Develop and share tips, indicators, warnings, information, and mitigation recommendations using established communications channels.
- Work with sector stakeholders to perform security audits, vulnerability, maturity and risk assessments and other infrastructure evaluations to determine weaknesses or vulnerabilities (technical, process, human resources, capabilities) and provide specialized assistance for remediation or mitigation.
- Develop and publish overviews of best practices for securing networks, systems and applications and education, training, and awareness programs.
- Promote and create training and information sharing activities to empower a specialized and well- trained cyber workforce in the UAE.

National Security Operations Centre (NSOC)

General tasks

- Collect information from sector-level incident management capabilities (e.g., Sector-specific SOCs and UAE aeCERT) and entity-specific CSIRTs, SOCs, and/or NOCs. Gather data feeds from continuous monitoring of networks.” and “Gather data and monitor cyber activity.
- Work to ensure stakeholders receive, and can act on, preventative and protective information. and Recommend proactive changes to information assets.
- Use predictive analysis tools to determine when an attack or incident might occur.
- Make alert and warning information available and highlight the emergence of critical changes in the overall state of UAE cyberspace.
- Encourage and supplement entity and sector-level risk and maturity assessments, training, and implement national preparedness trainings & exercises.

3.3 Detect

The Detect Phase outlines activities aimed at identifying, analyzing, investigating, escalating and reporting a cyber incident as well as organizing an initial response to it.

CII Entity

General tasks

- CII operators, leveraging their baseline SOC capabilities, are often the first to detect incidents on their networks and systems that may be of concern to their (or other) critical infrastructure sector(s) and the UAE, have credible threat intelligence pertaining to a potential activity or incidents or be aware of vulnerabilities that present a threat.
- Once suspicion arises, entities are to collect information about the observed activity, analyze for indicators of compromise, look for correlating information and perform additional research for the purposes of validation – as well as declare an incident if it is validated.
- Conduct appropriate initial incident response activities (containment) based on entity standard operating procedures, identify which resources have been affected or will be affected estimating the current and potential impact of the incident (impact assessment);
- Prioritize the incident based on impact assessment and categorize the incident based on guidelines and requirements provided in Annex 4.1 and inline with the Incident Response Framework.
- Document the investigation and gather evidence, including preparing information for escalation and reporting; and
- Report the incident in line with and based on guidelines, requirements and procedures provided in Annex 4.1 and inline with the Incident Response Framework.

3.3 Detect

Sector SOCs, aeCERT

General tasks

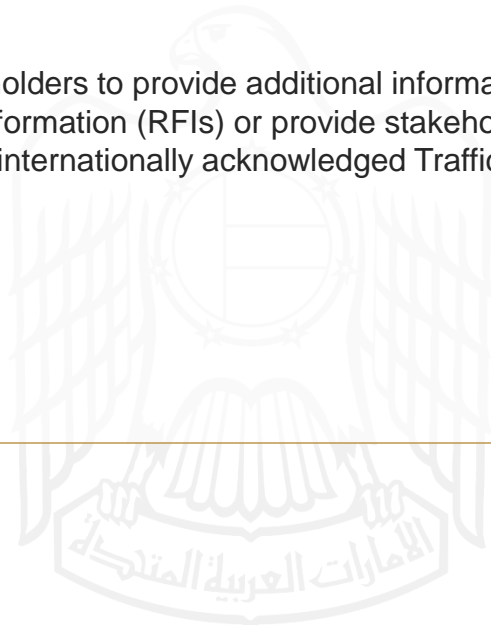
- Collect sector-wide information maintaining sector-level cyber situational awareness and analyze observed activity, analyze for indicators of compromise, look for correlating information, and perform additional research for the purposes of validation.
- Analyze available information on a sector-level building on entity-specific analysis, combining entity information with additional information from across the critical infrastructure sector.
- Categorize the incident based on guidelines and escalate to NSOC in line with reporting requirements.
- Conduct appropriate initial incident response activities (containment).
- Document the investigation and gather evidence, including preparing information for escalation and reporting.
- Report the incident in line with and based on guidelines, requirements and procedures provided in Annex 4.1 and inline with the Incident Response Framework.

3.3 Detect

National Security Operations Centre (NSOC)

General tasks

- Based on the common operational picture and available reporting, analyze observed or reported activity, analyze for indicators of compromise, look for correlating information, and perform additional research for the purposes of incident validation. National level analysis is built on entity- and sector-level input complemented by other information available to NSOC.
- Delivers an incident assessment and categorize the incident determining if one or more of the conditions on the national Cyber Incident Alert Schema have been met
 - Declare a Level 3 cyber incident if it is validated; or
 - In case It is needed , escalate by way of the NSOC Director making a recommendation to the NCRG Chair (CSC) to convene the NCRG with the relevant composition based on the nature and scope of the incident; or
 - In case It is needed , escalate by way of the NSOC Director making a recommendation to the CSC to raise the cyber incident level to Level 2 after coordination and consultation with NCEMA ; or
- Conduct appropriate initial incident response activities (containment) assisting affected sector SOCs and CII entities, including documenting activities and
 - Lead incident response during Level 3 cyber incident; or
 - Assist NCRG if a it is convened.
- NSOC may request relevant stakeholders to provide additional information by issuing documented requests for information (RFIs) or provide stakeholders with additional information following the internationally acknowledged Traffic Light Protocol (TLP).



3.4 Respond

The primary objective during the Respond Phase is first to contain the incident. Containment aims to prevent an incident to overwhelm resources, limit its impact, prevent it from spreading, and allow time for developing tailored remediation. After successful containment, eradication can take place eliminating components of the incident, including deleting malware and identifying and mitigating all vulnerabilities that were exploited.

CII Entity

During normal phase

- Maintain baseline operations, leverage their standard SOC capabilities in monitoring, assessment, and reporting.
- Monitor threat intelligence and continually enhance use cases
- Implement containment and eradication activities in line with their own SOPs and industry best practice.
- Acquire, preserve, secure and document evidence for investigation, corrective actions, potential disciplinary actions, and/or prosecution.

During Level 4 cyber incident

- Liaise with sector SOCs and NSOC through established channels enabling effective and timely communication, including responding to RFIs released by sector SOCs or NSOC to maintain the common operational picture and determine mitigation strategies.
- Implement mitigation strategies identified by the sector SOCs or NSOC to reduce the impact of the incident.

After significant incident declaration, during Level 3 cyber incidents

- Maintain effective and timely communication with NSOC, sector SOCs and the NCRG, including responding to RFIs and meeting incident reporting and information sharing requirements.
- Evaluate and execute mitigation strategies under the leadership and guidance of the NSOC as approved by the NCRG when convened.
- Maintain surge support for the foreseeable future.

1. Introduction

2. Incident Response Roles
and Responsibilities3. Cyber Incident
Response Plan

4. Appendices

3.4 Respond

Sector SOCs

Level 3 cyber incident

- Maintain effective and timely communication with NSOC and sector SOCs, including responding to RFIs and meeting incident reporting and information sharing requirements.
- Evaluate and execute mitigation strategies under the leadership and guidance of the NSOC.
- Maintain surge support for the foreseeable future.



1. Introduction

2. Incident Response Roles
and Responsibilities3. Cyber Incident
Response Plan

4. Appendices

3.4 Respond

National Security Operations Centre (NSOC)

During normal phase

- Maintain an up-to-date common operational picture and disseminate information in a leveraging standard reporting and information sharing through its liaison networks.

During Level 4 cyber incident

- Coordinate and implement containment and eradication activities on a national level and in cooperation with sector SOCs and assisting affected CII entities providing technical assistance.

After significant incident declaration, during Level 3 cyber incident

- Facilitate proper information flow and collaboration among partners as necessary through established channels, solicit status updates and maintain the common operational picture as per SOP, including maintaining relevant executive dashboards to the NCRG when convened.
- In cooperation with sector SOCs and affected CII entities evaluate and analyze available information and develop a technical Incident Response Plan to implement containment, mitigation and eradication activities on a national level and implement it after NCRG approval when convened.
- Provide periodic status reports and present the Incident Response Plan to the NCRG for its approval when convened.
- Provide logistical assistance and facilitate decision-making and assist oversight by the NCRG when convened.
- Conduct national crisis communication activities based on a documented Crisis Communication Plan following previously established communications approach tailored for Significant Cyber Incidents and approved by the NCRG, gathering, and disseminating controlled (if necessary sanitized and after instructions) information about the incident using appropriate channels, including liaison with national and international media.
- Provide with or deploy surge support (“fly-away teams”) to affected CII entities to assist incident response locally if necessary.

3.4 Respond

National Security Operations Centre (NSOC)

Level 2 cyber incident

- Facilitate proper information flow and collaboration among partners as necessary through established channels, solicit status updates and maintain the common operational picture as per SOP, including maintaining relevant executive dashboards to the relevant stakeholders.
- In cooperation with sector SOCs and affected CII entities evaluate and analyze available information and develop a technical Incident Response Plan to implement containment, mitigation and eradication activities on a national level and implement it after approval by CSC and relevant stakeholders.
- Provide periodic status reports and present the Incident Response Plan to the CSC and relevant stakeholders for its approval.
- Provide logistical assistance and facilitate decision-making and assist oversight by the CSC and relevant stakeholders .
- Conduct national crisis communication activities based on a documented Crisis Communication Plan following previously established communications approach tailored for Significant Cyber Incidents and approved by the CSC and relevant stakeholders , gathering, and disseminating controlled (if necessary sanitized and after instructions) information about the incident using appropriate channels, including liaison with national and international media.
- Provide with or deploy surge support (“fly-away teams”) to affected CII entities to assist incident response locally if necessary.



1. Introduction

2. Incident Response Roles
and Responsibilities3. Cyber Incident
Response Plan

4. Appendices

3.4 Respond

National Cyber Response Group (NCRG)

After significant incident declaration, Level 3 cyber incident

- Convene following previously established procedures.
- Review and request updates and RFIs, briefings by the NSOC and assess resource requirements necessary to manage the incident.
- Review, if necessary, adjust and approve the Incident Response Plan prepared by the NSOC.
- Review, if necessary, adjust and approve the Crisis Communication Plan.
- Based on the accepted Incident Response Plan guide, coordinate and oversee national response operations.
- Liaise with relevant stakeholders on a national level and mobilize national resources to mitigate the incident.



3.5 Recover

The Recovery Phase includes implementing appropriate remediation and restoration activities following the Incident Response Plan at CII entities and on a national level affected by an incident. The task at hand is to restore systems and operations to Normal state, confirm their consolidated functioning and remediate exploited or otherwise identified vulnerabilities to prevent similar incidents. For large-scale incidents, recovery may take months, thus the initial goal should be to increase the overall security with relatively quick, high-value changes to prevent future incidents.

Recovery activities should be conducted in a manner that preserves the integrity of the system and assists with an in-depth analysis and investigation of the incident, including meeting chain of custody and other evidence retention requirements enabling prosecution.

CII Entity

General Tasks

- CII operators are to meet all reporting and information sharing requirements, including responding to RFIs and providing periodic updates to relevant sector SOCs and the NSOC assisting with the maintenance of the common operational picture and providing an up-to-date view on the implementation of the Incident Response Plan.
- CII operators, leveraging their baseline SOC capabilities, are to implement remediation and restoration activities as outlined by the Incident Response Plan approved by and in cooperation with the NSOC, NCRG when convened and the relevant stakeholders to return affected systems and networks to Normal, Steady State.
- CII operators are to keep a detailed log of recovery and remediation actions and meet their legal or other mandatory chain of custody and other evidence retention obligations, including documentation.
- Reallocate resources from less vital missions to provide additional recovery capability, if necessary.
- Prepare an initial damage assessment including confirmation that the incident was closed, and all networks and systems operate normally.

1. Introduction

2. Incident Response Roles
and Responsibilities3. Cyber Incident
Response Plan

4. Appendices

3.5 Recover

Sector SOCs

General tasks

- Monitor sector level networks and assets, collect information, and inform the NSOC contributing to the maintenance of the common operational picture and the status of the implementation of the Incident Response Plan.
- Develop and provide input on cyber incident recovery for the NSOC to inform NCRG when convened and relevant stakeholders decision-making and assist in analysis and help remediation and recovery activities at an entity and sector level including allocating available surge support.

National Security Operations Centre (NSOC)

General tasks

- Monitor incident management and collect information maintaining an up-to-date common operational picture.
- Manage and overview the implementation of appropriate technical remediation and restoration activities following the Incident Response Plan on a national level providing technical expertise and surge support to sector SOCs and CII operators or government organizations to assist in the restoration of critical networks and services.
- Close the incident as appropriate and communicate Cyber Incident Alert Level (incl. de-escalation) on a national level and to relevant stakeholders.
- Carry out communication tasks as per SOP and following the Crisis Communication Plan.
- Prepare an initial damage assessment.

1. Introduction

2. Incident Response Roles
and Responsibilities3. Cyber Incident
Response Plan

4. Appendices

3.5 Recover

National Cyber Response Group (NCRG)

General tasks

- The NCRG is to coordinate and overview the implementation of the Incident Response Plan on a strategic level, including remediation and restoration activities on a national level during a Level 3 cyber Incident. This includes coordination of relevant stakeholders, mobilization of surge and national support.
- Overview the implementation of the Crisis Communication Plan.
- Overview the preparation of the initial damage assessment.



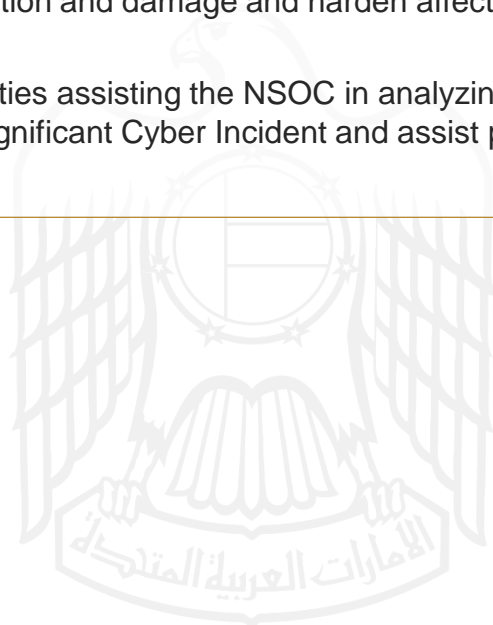
3.6 Learn and Improve

The Learn and Improve Phase is the last element of the cyber incident management lifecycle to be implemented after an incident is closed. This Phase aims to collect and analyze information to understand what happened, why it happened, and come up with a plan outlining recommendation for improvement and mitigation making sure that the same incident cannot happen, vulnerabilities are mitigated, and the overall cybersecurity posture of the UAE is enhanced.

CII Entity

General tasks

- Collect and, in cooperation with sector SOCs and the NSOC, analyze both available data and processes to assess what happened, determine attribution if possible, develop and update threat profiles and produce a Post-Incident Report documenting findings, including an impact and detailed damage assessment, identified deficiencies and mitigating measures and improvements concerning processes and policies.
- Implement recommendations outlined in the Post-Incident Report remediating vulnerabilities to avoid future disruption and damage and harden affected networks and systems.
- Participate in lessons learned activities assisting the NSOC in analyzing and addressing the root cause of the Significant Cyber Incident and assist prosecution if relevant.



1. Introduction

2. Incident Response Roles
and Responsibilities3. Cyber Incident
Response Plan

4. Appendices

3.6 Learn and Improve

Sector SOC's

General tasks

- Carry out a sector-level post-mortem, including root cause analysis after the incident conducting a detailed post-incident assessment to evaluate response activities, identifying strengths and weaknesses, and modifying and creating new operational procedures as part of a continuous and adaptive learning environment. Use post-incident report data to inform process improvements.
- Inform and support knowledge transfer among CII entities, regulators and the NSOC including the development of possible incident scenarios for future exercises.
- Model the impact of incidents across a given individual sector conduct trend analysis to understand and predict future trends and high-risk scenarios.

National Security Operations Centre (NSOC)

General tasks

- Conduct lessons learned activities in collaboration with the NCRG and relevant stakeholders as appropriate and carry out a national-level post-mortem, including root cause analysis after the incident assessing response activities and adjusting processes as part of a continuous and adaptive learning environment.
- Lead attribution efforts on a national level and collaborate with relevant partners in follow-up activities, including prosecution as appropriate.
- Facilitate knowledge transfer among stakeholders of the UAE cyber ecosystem and issue recommendations to CII entities, sector SOC's and policymakers.
- Model the impact of incidents on a national level, including assessments of interdependencies and conduct trend analysis to understand and predict future trends and high-risk scenarios.

3.6 Learn and Improve

National Cyber Response Group (NCRG)

General tasks

- Evaluate the performance of national cyber incident management capabilities, including processes and policies.
- Conduct lesson learned activities after a level 3 cyber Incident to review the root cause and its potential or actual impact to operations and the UAE cyber ecosystem.
- Recommend enhancements or adjustments to the CIRP, UAE policies and the UAE cyber incident response capability.



The background features a complex network of thin, light-colored lines connecting various nodes. Some nodes are represented by small circles, while others are larger, irregular shapes in shades of green and yellow. On the right side, there are vertical lines resembling a circuit board with small circles at intervals. A large, solid black rectangle is positioned in the lower-middle part of the page, containing the section title.

SECTION 4
APPENDICES

1. Introduction

2. Incident Response Roles
and Responsibilities3. Cyber Incident
Response Plan

4. Appendices

4.1 Cyber Incident Alert Schema

The Cyber Incident Alert Schema operates as a national-level alert and warning mechanism. This mechanism conveys information on current cyber incidents and their level of impact to Critical Information Infrastructure (CII) sectors, entities and government organizations of the United Arab Emirates.

The Schema is to convey information in a condensed form to key stakeholders through four alert levels (level 4, level 3, level 2 and ;level 1). The alert level will consider the actual cyber activity and its potential to escalate, its impact to CII sectors of the UAE and its effect on response capabilities. All-in-all alert levels are designed to contribute to overall cyber situational awareness providing an indication of the cyber incident status and impact in the UAE.





1. Introduction	2. Incident Response Roles and Responsibilities	3. Cyber Incident Response Plan	4. Appendices
-----------------	-------------------------------------------------	---------------------------------	----------------------

4.1 Cyber Incident Alert Schema

Table 1: National Cyber Incident Alert Levels

	Alert level	Activity	Impact
Significant Cyber Incident	Level 1 Highest-level impact	<ul style="list-style-type: none"> Threat of, or actual, malicious cyber activity that will disrupt, destroy, or degrade CII and/or government systems exists. Incident occurred, is imminent, or is ongoing. 	<ul style="list-style-type: none"> Potential or observed total or near-total destruction, degradation, or compromise of CII across one or more sectors. Potential or observed serious and widespread degradation or destruction, threatening continued operation of government or CII sector. Normal business operations and functions may be indefinitely suspended. Potential impact is managed by the NCEMA.
	Level 2 High-level impact	<ul style="list-style-type: none"> Threat of, or actual, increased malicious cyber activity directed at national critical services exists. Known or expected targeted intrusion or exploit of a CII providing a national critical service is present. 	<ul style="list-style-type: none"> Potential for or observed major degradation, disruption and/or destruction of or damage to CII across one or more sectors. Potential impact is managed by the NCEMA.
	Level 3 Medium-level impact	<ul style="list-style-type: none"> Threat of, or actual, elevated malicious cyber activity exists. Known or expected intrusion or focused attack is present. 	<ul style="list-style-type: none"> Potential for or observed compromise and/or degraded service in one or more CII sectors. Potential for or observed elevated level of degradation, disruption or damage. Potential impact is managed by the NSOC and NCRG when needed.
Steady-state	Level 4 Low-level impact	<ul style="list-style-type: none"> Threat of, or actual, malicious cyber activity presents only a general concern. 	<ul style="list-style-type: none"> CII sectors or government systems are not targeted or affected. Potential impact is manageable by the responsible owner/operator.

1. Introduction

2. Incident Response Roles
and Responsibilities3. Cyber Incident
Response Plan

4. Appendices

4.2 UAE Sample IRPs – Typical attack scenarios and playbooks

CSC and NSOC is mandated to lead national cyber incident response in the UAE. In implementing that mandate as lead national agency, CSC/NSOC is committed to prepare the UAE incident response community for major cyber incidents to protect the nation's critical cyber assets. One way to increase preparedness, based on international best practice, is to develop Incident Response Playbooks. The goal of such efforts is to model typical, globally observed attack scenarios to plan ahead, enhance preparedness, test processes and approaches. The below are intended only as high-level models for IRPs as much more detailed plans can be established and refined during exercises involving key actors. Such projects can contribute significantly to cyber preparedness and raise awareness among high-level decision-makers. The aim of these IRPs is not to delve into minuscule technical detail, but to model and test national response from a 'whole-of-government' perspective provides a standardized response process for cybersecurity incidents and describes the process and completion through the incident response phases including indication of whether a stage forms technical or governance part of incident response.

While the below scenarios are fictional, they all were developed based on real, historical cyberattacks that caused massive loss. The three playbooks below can also be considered as model use cases for a national incident response capability outlined below in growing severity.





1. Introduction

2. Incident Response Roles
and Responsibilities3. Cyber Incident
Response Plan

4. Appendices

4.2 UAE Sample IRPs – Typical attack scenarios and playbooks

4.2.1 Attack Scenario I – Conventional Power Plant suffers Ransomware Attack

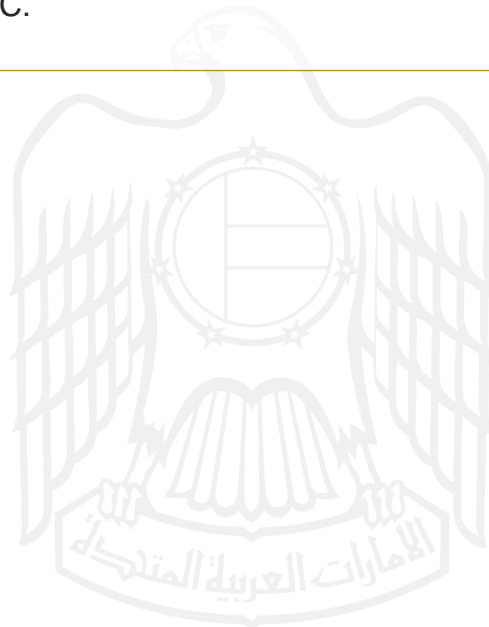
CII entity (fictional): UAE Power Plant (MPP)

Scenario description: In the early hours during the Eid Al Fitr Holiday UAE PP personnel and national grid operators record decreased output by MPP. Soon MPP CII SOC personnel receives initial SIEM malware alerts. During the subsequent three hours several critical IT systems (prod) of UAE PP becomes unavailable or stop functioning.

Incident Response Process

Detect

- [technical] Based on SIEM alerts and initial investigation MPP CII SOC declares an incident (malware attack), start to collect evidence (incident indicators, TTPs, attack signatures – see SOC Baseline and Reporting and Sharing requirements and conduct initial analysis.
- [governance] Based on its initial analysis and leveraging the Cyber Incident Alert Schema CII SOC initially classifies the incident as at Level 3 and subsequently escalates the incident to Sector SOC.



1. Introduction

2. Incident Response Roles
and Responsibilities3. Cyber Incident
Response Plan

4. Appendices

4.2 UAE Sample IRPs – Typical attack scenarios and playbooks

Incident Response Process

Respond

- [governance] Based on available information and leveraging the Cyber Incident Alert Schema Sector SOC declares 'Level 3' incident.
- [technical] Sector SOC (following up on the protocol outlined by the CIRP and detailed SOPs) reports and shares information with NSOC that serves as a national fusion centre on cyber incident management maintaining the common operational picture.
- [technical] CII SOC with assistance from Sector SOC Initiates response activities based on prepared playbooks aiming to contain and mitigate the attack.
- [technical] CII SOC report incident updates according to requirements (outlined in Appendix A and SOC Baseline).
- [technical] Sector SOC reports incident information to NSOC as per sharing and reporting requirements.
- [governance] NSOC informs and liaises with NCEMA.
- [governance] NCEMA is leading incident response out of cyber scope.

Recover

- [technical] CII SOC with assistance from Sector SOC implements DR and BCP plans and successfully contain the attack, execute eradication plan then recover affected assets in a few hours.
- [governance] Sector SOC closes incident.

Learn and Improve

- [technical] and [governance] CII SOC prepares documentation collecting relevant evidence, post incident analysis and lessons learned (incl. hardening steps). Documentation is shared with Sector SOC.
- [technical] and [governance] Sector SOC shared lessons learned with other members of the CII Sector via established ISC channels (see Information Sharing Framework).



1. Introduction	2. Incident Response Roles and Responsibilities	3. Cyber Incident Response Plan	4. Appendices
-----------------	-------------------------------------------------	---------------------------------	----------------------

4.3 List of cyber security-related UAE Policies and Standards

The below policies and standards form the overall governance policy framework for the cyberspace of the United Arab Emirates:

Authority/Body	Document
CSC	UAE IA Regulation
CSC	UAE Critical Information Infrastructure Policy
CSC	UAE National Cybersecurity Risk Management Framework
CSC	UAE National Cyber Security Strategy (2019)





1. Introduction

2. Incident Response Roles
and Responsibilities3. Cyber Incident
Response Plan

4. Appendices

4.4 Acronyms

Usage	Description
aeCERT	Computer Emergency Response Team of the UAE
CII	Critical Information Infrastructure
CIIP	Critical Information Infrastructure Protection
CSC	Cyber Security Council of the UAE
NCEMA	National Crisis and Emergency Management Authority
CIRF	Cyber Incident Response Framework
NCRG	National Cyber Response Group
CIRP	Cyber Incident Response Plan
NCSGF	National Cybersecurity Governance Framework
NCSS	National Cybersecurity Strategy

