الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

National Policy for Managed Security Operations Centers (MSOC)

(NPMSOC-1:2024)

TLP: White

Document Classification: Public

In the Name of Allah,
The Most Gracious,
The Most Merciful

DISCLAIMER: The following policy will be governed by and implemented in accordance with the laws of the Kingdom of Saudi Arabia, and must be subject to the exclusive jurisdiction of the courts of the Kingdom of Saudi Arabia. Therefore, the Arabic version will be the binding language for all matters relating to the meaning or interpretation of this document

Traffic Light Protocol (TLP):

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

- Red – Personal, Confidential, and for the Intended Recipient Only
  The recipient has no right to share information classified in red with any person outside the defined range of recipients, either inside or outside the organization, beyond the scope specified for receipt.

- Amber – Restricted Sharing
  The recipient may share information classified in amber only with intended recipients inside the organization and with recipients who are required to take action related to the shared information.

- Green – Sharing within the Same Community
  The recipient may share information classified in green with other recipients inside the organization or outside it within the same sector or related to the organizations. However, it is not allowed to exchange or publish this information on public channels.

- White – No Restrictions

Table of Contents

Page

1. Introduction

The National Cybersecurity Authority (NCA) is the national entity in charge of cybersecurity in the Kingdom of Saudi Arabia, and serves as the national authority and reference on its affairs. The NCA aims to improve the cybersecurity posture of the kingdom in order to safeguard its vital interests, national security, critical infrastructures, high-priority sectors, and government services and activities, according to its mandate that was approved by Royal Order number 6801, dated 11/2/1439 AH. The NCA mandate includes, but not limited to: development of cybersecurity national policies, governance mechanisms, frameworks, standards, controls, and guidelines; as well as circulating them with relevant stakeholders, following up on their compliance, and updating them. In addition, the NCA mandate includes licensing individuals and non-governmental organizations to practice cybersecurity activities and operations as determined by NCA, as well as stimulating cybersecurity sector growth in the Kingdom and encouraging innovation and investment in it.

The NCA has issued this policy to achieve its mandate based on the second phase of the NCA strategy (2.0) and its initiatives, such as developing national cybersecurity regulations, and building advanced cybersecurity monitoring, detection and information sharing capabilities ecosystem.

2. Definitions

The terms used in this policy will have the same meanings as stated in the table below, unless the context requires otherwise:

Term	Definition
NCA	National Cybersecurity Authority.
Organization	A public/government, private for-profit, private non-profit, or any other form of organization.
Policy	National Policy for the Managed Security Operations Centers, issued by the NCA.
Framework	The Regulatory Framework for Licensing MSOC Services, issued by the NCA.
Critical National Infrastructure (CNI)	Basic elements of the infrastructure, such as (assets, facilitates, systems, networks, processes, key employees responsible for the operation and processing of such elements) that the loss of which or being subject to security breaches would lead to: 1- Significant negative impact on the availability, integration or delivery of basic services, including services that if subjected to risk would lead to significant losses in property and/or lives and/or injuries, considering the economic and/or social implications. 2- Significant impact on the National Security and/or National Defense and/or State economy or national capabilities
Security Operations Center (SOC)	It is a center that provides cybersecurity events monitoring operations services for the organization's technology ecosystem, which can detect cyber threats, find out how they occur, and provide recommendations, as well as solutions and necessary measures to contain such threats.
Managed Security Operations Center (MSOC) Services	These are the services that the beneficiary organization receives from the service provider in order to monitor cybersecurity events in its technology ecosystem to detect cyber threats, know how they occur, and provide recommendations on how to address them by the beneficiary. These services include processes, staffing, systems, etc.
Beneficiary	Any organization that contracts with the service provider, for the purpose of obtaining MSOC services.
Service Provider	A licensed organization by the NCA to provide MSOC services in the Kingdom of Saudi Arabia, according to the Regulatory Framework for Licensing MSOC Services, issued by the NCA.

3. Policy Objectives

This policy aims to realize the following:

1. Enhancing cybersecurity situational awareness at the organizational and national level.
2. Enabling organizations in the Kingdom to obtain high quality trusted and mature MSOC services, in a manner that achieves its purpose.
3. Stimulating the growth of the cybersecurity sector in the Kingdom and promoting innovation and investment in it, by creating an organized work environment and reducing the gap between supply and demand in cybersecurity services.
4. Improving cybersecurity spending efficiency at the national level.

4. Policy Scope

This policy applies to the following organizations:

A. Government organizations, including ministries, authorities, establishments, centers, councils, committees, secretariats and others, as well as their companies and entities

B. Private sector organizations owning, operating or hosting critical national infrastructures (CNIs).

C. Any other organizations required by the NCA to implement this policy, at its absolute discretion, to achieve relevant national targets.

The NCA encourages all other organizations in the Kingdom that are not in scope of paragraphs (A), (B) and (C) above, to contract a service provider to obtain Managed Security Operations Center (MSOC) services based on their cybersecurity needs.

5. Policy Clauses

All organizations which are obligated to implement this policy shall comply with the following:

5.1 Adhering to all regulatory provisions, decisions and directions issued by the NCA in accordance with its mandate as the national authority and reference in all matters related to cybersecurity in the Kingdom.

5.2 Obtaining the NCA's prior approval for any initiatives, projects or services related to the Security Operations Center (SOC), whether the initiative is at the organizational, sectorial, or any other level.

5.3 Carrying out the organization's SOC work through a Tier 1 licensed Managed Security Operations Center (MSOC) service provider, in accordance with the framework, for all MSOC services as outlined in the Appendix.

6. Compliance Procedures to the Policy Clauses

All organizations which are obligated to implement this policy shall comply with the following procedures:

6.1 Providing the NCA - according to the specified form - with a report that includes the following:

6.1.1. The current status of all the organization's SOC work, including technologies, procedures, staffing, etc.

6.1.2. A plan to comply with the policy clauses, which includes, as the case may be: a corrective plan to move from contractual obligations with the current entity providing MSOC services to a Tier 1 licensed MSOC service provider according to the framework; or a corrective plan to move from the organization's in-house SOC to a Tier 1 licensed MSOC service provider according to the framework.

6.2 The NCA shall be provided with the report referred to in paragraph (6.1) within a maximum of (90) days from the effective date of this policy through the NCA specified communication channels.

6.3 The NCA shall be immediately informed upon the completion of the organization's SOC transfer to a service provider.

6.4 The NCA will review the reports received, pursuant to this clause, and will inform the concerned organization of the report approval, request for amendment, or any additional relevant requirements.

7. General Provisions

7.1 The NCA, at its absolute discretion and pursuant to sector regulation interests, may impose additional conditions or requirements, or cancel existing ones, on organizations which are obligated to implement this policy.

7.2 The policy provisions will be enforced starting from the date the policy was published in NCA website.

7.3 The NCA will review this policy and update it whenever is needed. Pursuant to sector regulation requirements, organizations which are obligated to implement this policy shall comply with any policy update.

7.4 Organizations which are obligated to implement this policy must adhere to all NCA templates and deadlines.

8. Appendix

MSOC Services

MSOC services are services provided to the beneficiary organization from a service provider, to monitor cybersecurity events in the technology ecosystem of the beneficiary organization to detect cybersecurity threats, understand how they occur, and provide recommendations on how to address them in order to implement these recommendations by the beneficiary. These services include operations, staffing, systems, etc.

Below is a description of the minimum MSOC services that organizations can obtain from a service provider according to this policy:

1. Threat Monitoring and Detection

This involves providing a continuous monitoring service for the technology ecosystem of the national beneficiary, including the organization's networks and systems, early detection of cybersecurity threats and attacks, and issuing alerts via monitoring and detection tools using different detection methods, such as pre-defined detection use-cases, indicators of compromise, and detection rules, and classifying alerts according to their severity. This is in addition to issuing immediate alerts to the beneficiary about detected threats, and periodic technical and executive reports on the state of cybersecurity, by managing and operating cybersecurity tools specialized in monitoring and detection.

2. Threat Analysis and Investigation

This involves analyzing and investigating the detected alerts, linking the various events and understanding them within the context of the beneficiary's ecosystem. It also includes identifying the true alerts related to actual cybersecurity incidents and identifying false alerts based on a systematic method of analysis of all threats. In addition, this service involves providing the national beneficiary with initial and in-depth analysis including the causes of alerts and incidents. The service also includes conducting a sweeping and threat hunting exercises, as well as conducting analysis and investigation into cases that the national beneficiary has reported to the service provider.

3. Threat Containment Recommendations

This involves providing integrated and effective recommendations to the national beneficiary on how to contain and neutralize cybersecurity threats, to be applied by the beneficiary to control the risks of the detected threats and attacks.


الهيئة الوطنية
للأمن السيبراني
National Cybersecurity Authority