الهيئـــة الوطنيـــة
للأمـــن السيبـــراني
National Cybersecurity Authority

National Policy for Managed Security Operations Centers (MSOC)

(Public Consultation)

Sharing Notice: White	
Document Classification: Public	

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

Traffic Light Protocol (TLP):

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

🔴 Red – Personal, Confidential and for Intended Recipients Only

The recipient has no rights to share information classified in red with any person outside the defined range of recipients either inside or outside the organization.

🟠 Amber – Restricted Sharing

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

🟢 Green – Sharing within The Same Community

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

○ White – No Restriction

Contents

1. Introduction

The National Cybersecurity Authority (NCA) is the national entity in charge of cybersecurity in Saudi Arabia and serves as the national authority on its affairs. The NCA aims to improve the cybersecurity posture of the country in order to safeguard its vital interests, national security, critical infrastructures, high-priority sectors, government services and activities in accordance with its regulation under Royal Decree number (6801) dated 11/2/1439 A.H. The NCA's mandate includes introducing cybersecurity policies, governance mechanisms, frameworks, standards, controls, and guidelines; as well as circulating them with relevant stakeholders, following up on their compliance, and updating them. Cybersecurity monitoring over assets requires continuous, round-the-clock operations without interruption, as well as taking the necessary measures when detecting any activities or threats to those assets, in addition to the fact, that national entities have varying capabilities in this aspect. This framework comes to organize this sector in a way that contributes to enhancing cybersecurity for entities, as well as at the national level.

2. Definitions

The terms used in this policy shall have the following meanings, unless the context requires otherwise:

Term	Definition
NCA	National Cybersecurity Authority.
Organization	A public, private for-profit, private non-profit, or any other form of organization.
Critical national infrastructure (CNI)	These are the assets (i.e. facilities, systems, networks, processes, and key operators who operate and process them), whose loss or vulnerability to security breaches may result in: 1) Significant negative impact on the availability, integration or delivery of basic services, including services that could result in serious loss of property and/or lives and/or injuries, alongside observance of significant economic and/or social impacts. 2) Significant impact on national security and/or state economy or national capacities.
License	A document issued by NCA for natural or legal persons in order to provide or develop cybersecurity services, products, and solutions in Saudi Arabia, or for individuals to practice cybersecurity-related activities and operations, as determined by NCA.
Security Operations Center (SOC)	A combination of people, processes, and technologies specialized in monitoring networks, IT systems, operational technologies, or its components of hardware or software, services, or data. As well as detecting anomalies, threat analysis and containment.
Managed SOC (MSOC)	A Center that aims to monitor the cybersecurity state in the technical ecosystem of the beneficiary, for the early detection of cyber threats, discovering how they occur, and providing comprehensive recommendations on how to address them and take the necessary measures to contain them. The business model includes a contract between the beneficiary and the managed services provider, to take full responsibility of cybersecurity monitoring activities including operations, staff and systems in accordance to Appendix A.
Managed SOC (MSOC) Service Provider	An organization providing managed SOC services.

3. Objectives of the National Policy for Managed Security Operations Centers (MSOC)

The purpose of the Policy is to enable organizations in Saudi Arabia to obtain mature MSOC services as well as increase situational awareness at the organizational and at the national level, ensure high quality and consistent MSOC services for organizations, enable information sharing between SOCs and across the entire ecosystem, and improve expenditure efficiency in cybersecurity at the national level. As cyber monitoring operations of assets are required to run continuously around the clock without interruptions, while taking the necessary measures when discovering any activities or threats against those assets. This policy comes to regulate this field in a way that contributes to enhancing cyber security for organizations, and on the national level.

4. National Policy for Managed Security Operations Centers (MSOC) Scope

This policy mandates government organizations in the Kingdom of Saudi Arabia (including ministries, authorities, establishments and others) and its companies and entities, as well as private sector organizations owning, operating or hosting Critical National Infrastructures (CNIs), in addition to any other specific organizations that NCA has mandated, to use one or multiple licensed MSOCs service providers to cover the SOCs services, as outlined in Appendix A.

5. National Policy for Managed Security Operations Centers (MSOC)

All organizations, covered by the scope of this Policy, will be required to use Tier 1 licensed MSOC service provider for all services related to SOCs, as stipulated in Appendix A. This mandate will take effect on October 1, 2023. The remaining articles of this policy list all obligations, procedures, and additional stipulations.

While the Policy mandates all organizations covered by the scope thereof, the NCA reserves the right to mandate any other non-CNI organizations as part of this policy at NCA's discretion. All other organizations that are not mandated to follow the provisions outlined in this document are strongly advised to retain the services of licensed Tier 1 or Tier 2 MSOCs service providers based on their cybersecurity needs. If these other organizations opt to retain the services of MSOCs service provider, they are mandated to use NCA licensed MSOCs service providers.

6. Obligations of Organizations

All organizations covered by this Policy must comply with the provisions thereof, all relevant NCA regulatory provisions, relevant regulations, the laws of Saudi Arabia, and the following obligations:

6.1 Comply with the regulations, acts, decision, and instructions related to cybersecurity in force in Saudi Arabia.

6.2 Convert to a Tier 1 licensed MSOCs service provider, with regard to SOCs services, in accordance with the provisions outlined in the Regulatory Framework for MSOCs licensing.

6.3 Submit a situational analysis report explaining the current situation of their SOCs, as defined in Appendix B, to NCA within the period determined by the NCA.

6.4 Submit a “Roadmap to Compliance” report to be reviewed and approved by the NCA, as outlined in Appendix B, to NCA within the period determined by the NCA.In relation to organizations that are not able to meet the timeline and process stipulated in their NCA approved transition plan, they are required to submit an updated “Roadmap to Compliance” report, as stipulated in Appendix B. Such report shall be quarterly updated, until the organization is fully compliant with this policy.

6.5 Notify the NCA once the organization completes its transition to a Tier 1 licensed MSOCs service provider.

7. General provisions

NCA reserves the right to amend, modify, and/or delete any part of this policy, at its discretion.

8. Appendices

Appendix A

Additional Information on the services provided by MSOCs

Managed services aim to monitor the cybersecurity state in the technical ecosystem of the beneficiary, with the objective of early detection of cyber threats, discovering how they occur, and providing comprehensive recommendations on how to address them and take the necessary measures to contain them. The business model includes a contract between the beneficiary and the managed services provider, to take full responsibility for cybersecurity monitoring activities including operations, staff and systems. Such services are provided remotely. The following is a description of key services provided by MSOCs:

1. Continuous Threat Monitoring and Detection

This service includes providing (24/7) continuous and real-time monitoring of the beneficiary's technical ecosystem (including its networks and systems), and early detection of cyber threats and attacks. It also includes issuing alerts triggered through monitoring and detection tools that use several detection methods, including detection use-cases, Indicators of Compromise, and Detection rules. Additionally, this services includes classifying alerts based on its severity, issuing instant alerts on threats targeting beneficiary, and developing executive and technical reports on the state of cybersecurity by managing and activating cybersecurity monitoring and detection tools.

2. Threat Analysis and Investigation

This service includes analyzing and investigating detected threats, linking several events and putting them into the context of the beneficiary's ecosystem. It also supports the beneficiary in identifying accurate alerts related to real cyber incidents, and identifying false alerts based on a systematic method in analyzing all threats. Through this service, the beneficiary will be provided with anlytical reports that include full analysis of cyber incidents' and alerts' root causes. Additionally, this service includes several capabilities, including sweeping, threat hunting, and the ability to analyze and investigate cases reported by the service provider.

3. Threat Containment

This service includes providing comprehensive and effective recommendations to the beneficiary, including how to contain and neutralize cyber threats, which can be applied by the beneficiary's internal teams to control the risk of detected cyber attacks, threats and incidents.

Depending on the scope of work and service level agreement, this service may include the service provider performing the containment of cyber threats -if possible- and implementing the necessary measures for that, including isolating endpoints targeted by threats and attacks from the beneficiary's system.

Appendix B

Documents for submission to NCA

Organizations shall submit a situation analysis report explaining the current situation of their SOCs. In addition, organizations shall also submit a "Roadmap to Compliance" report which documents the organization's transition plan to comply with this policy.

All organizations shall submit this report attached with supporting documents, such as cybersecurity strategies, procedures, and guidelines.

1. Current Status Analysis Report

All organizations covered by this policy will be required to submit a Current Status Analysis Report to the NCA outlining the coverage of SOCs services. This report must outline all SOCs services, and how these are being managed, as well as who is responsible for providing these services.

This document must include the following SOCs services sections:

1. Threat monitoring and detection
2. Threat analysis and investigation
3. Threat containment

For every section above in the situational analysis report, the organization covered by the scope of this policy must address the following questions:

1. Is the SOC service being covered through an agreement with a licensed MSOC service provider?
2. Who is the service provider?
3. Is the organization covered by this policy requesting an extension for this MSOC service? If so, what is the reason?
4. If the organization is covering the SOC service internally, through the organization's own resources, what are the resources being allocated to provide this SOC service? How is the organization managing the SOC service and ensuring quality?
5. What are the current risks facing the organization for covering the SOC service internally? What is the organization's mitigation plan?

In addition to addressing these questions, the organization covered by this policy must attach additional supporting documents as part of its report, as appropriate. In some cases, the organization must provide information about technical specifications, historical activity and investments, and background of information security staff.

At the discretion of the NCA, the organization covered by this policy may be required to provide an updated version of this report.

2. Roadmap for compliance

Organizations covered by the scope of this policy are required to create a roadmap of compliance based on the situational analysis report. The roadmap has to outline the time it will take the organization to transition to a Tier 1 licensed MSOC provider. Targets within the roadmap are required to be listed on a quarterly basis, at the discretion of the NCA, although organizations are free to form targets at a quarterly or monthly basis, or any time period that is deemed appropriate.

Elements that need to be included in the roadmap are:

1. Project plan and timeline to integrate to licensed MSOC service provider, based on requirements, sophistication of the process, and any other relevant factors.
2. Section on potential challenges faced by the organization covered by this policy as a result of complying with it.

All documents must be submitted through channels dedicated by NCA.

الهيئـــة الوطنيـــة
للأمـــن السيبـــراني
National Cybersecurity Authority