National Communications Authority (NCA)

Somalia Computer Emergency Response Team (SOMCERT)

SOMCERT POLICIES

2021

1. General Policies of SOMCERT

Computer and information security is critical to any government, private, or individual, from both public and private organizations. Everyone depends on information technology and information systems to successfully carry out their missions and business functions. Information systems are subject to threats including incidents and events that can have an adverse effect on organizational operations, assets, individuals, other organizations, and the Somali Government when both the known and unknown vulnerabilities are exploited compromising the confidentiality, integrity or availability of the information being processed, stored, or transmitted by these systems. It is important that these threats are detected and reported at earlier stages and those agency heads at all levels understand their responsibilities.

2. SOMCERT Documentation Policy

a) All documents of different forms whether written, spoken or recorded electronically or printed, shall be protected from accidental or intentional unauthorized modification, destruction, or disclosure throughout its life cycle.

b) All policies and procedures shall be documented and made available to individuals responsible for their implementation and compliance.

c) All documentation, which include electronic form, shall be retained for at least six (6) years after its last revision pertaining to policies and procedures, after changes have been made or if any specific policies on records archiving and disposition provide a retention period different from that established by the records disposition schedule of the organization, the retention period established by law or regulation shall govern.

d) All documentation shall be periodically reviewed at regular intervals to ensure its continued appropriateness and applicability over a period of time.

3. SOMCERT Accountability Policy

a) It is the policy of Cyber Security Department in collaboration with Ministry of Communications and Technology (MoCT) to ensure the integrity and reliability of the government's digital presence and corporate identity as part of its commitment to good governance. The Cyber Security Department shall provide a cost-efficient service and set of standards, which shall serve as means for actors both within and outside of government to enforce and accountability.

b) Establish control in reporting all computer emergency incidents and events through

appropriate channels with the creation of the SOMCERT.

4. Establishing SOMCERT Policy

a) National Communications Authority (NCA) is mandated to establish SOMCERT under Cyber Security Department to assign individuals dedicated to work as full-time members.

b) Establish the guidelines for handling reported computer emergency incidents and events.

c) Computer emergency incidents and events shall be classified for information systems based on the potential impact on an organization in the event of incidents which endanger the information.

d) Processes and procedures established by Cyber Security Department for detecting and reporting the occurrence of information security events shall be implemented and observed accordingly.

e) All reported incidents must be identified to initiate immediate response actions to deal with the information security incident.

f) All incident reports shall be updated and collected into the SOMCERT database.

g) All incidents that have been resolved or closed must be reviewed.

h) Review outputs from SOMCERT for process improvement.

5. Incident Prioritization Policy

Prioritizing the handling of the incident is perhaps the most critical decision point in the incident handling process. Incidents should not be handled on a first-come, first-served basis as a result of resource limitations. Instead, handling should be prioritized based on the relevant factors, such as the following:

- **Functional Impact of the Incident.** Incidents targeting IT systems typically impact the business functionality that those systems provide, resulting in some type of negative impact to the users of those systems. Incident handlers should consider how the incident will impact the existing functionality of the affected systems. Incident handlers should consider not only the current functional impact of the incident, but also the likely future functional impact of the incident if it is not immediately contained.
- **Information Impact of the Incident.** Incidents may affect the confidentiality, integrity, and availability of the organization's information. For example, a malicious agent may exfiltrate sensitive information. Incident handlers should consider how this information exfiltration

will impact the organization's overall mission. An incident that results in the exfiltration of sensitive information may also affect other organizations if any of the data pertained to a partner organization.

- **Recoverability from the Incident.** The size of the incident and the type of resources it affects will determine the amount of time and resources that must be spent on recovering from that incident. In some instances it is not possible to recover from an incident (e.g., if the confidentiality of sensitive information has been compromised) and it would not make sense to spend limited resources on an elongated incident handling cycle, unless that effort was directed at ensuring that a similar incident did not occur in the future. In other cases, an incident may require far more resources to handle than what an organization has available. Incident handlers should consider the effort necessary to actually recover from an incident and carefully weigh that against the value the recovery effort will create and any requirements related to incident handling.

Functional Impact Categories

Category	Definition
None	No effect to the organization's ability to provide all services to all users
Low	Minimal effect; the organization can still provide all critical services to all users but has lost efficiency
Medium	Organization has lost the ability to provide a critical service to a subset of system users.
High	Organization is no longer able to provide some critical services to any users

Information Impact Categories

Category	Definition
None	No information was changed, deleted, or otherwise compromised
Privacy Breach	Sensitive personally identifiable information (PII) of taxpayers, employees, beneficiaries, etc. was accessed
Proprietary Breach	Unclassified proprietary information, such as protected critical infrastructure information (PCII) was accessed
Integrity Loss	Sensitive or proprietary information was changed or deleted

6. Coordination Relationships Policy

An incident response team within an organization may participate in different types of coordination arrangements, depending on the type of organization with which it is coordinating. For example, the team members responsible for the technical details of incident response may coordinate with operational colleagues at partner organizations to share strategies for mitigating an attack spanning multiple organizations. Alternatively, during the same incident, the incident response team manager may coordinate with national and International organizations to satisfy necessary reporting requirements and seek advice and additional resources for successfully responding to the incident. The following table will provide coordination relationships that may exist when collaborating with outside organizations.

Category	Definition	Information Shared
Team-to Team	Team-to-team relationships exist whenever technical incident responders in different organizations collaborate with their peers during any phase of the incident handling life cycle. The organizations participating in this type of relationship are usually peers without any authority over each other and choose to share information, pool resources, and reuse knowledge to solve problems common to both teams.	The information most frequently shared in team-to team relationships is tactical and technical (e.g., technical indicators of compromise, suggested remediation actions) but may also include other types of information (plans, procedures, lessons learned) if conducted as part of the Preparation phase.
Team-to coordinating team	Team-to-coordinating team relationships exist between an organizational incident response team and a separate organization that acts as a central point for coordinated incident response and management. This type of relationship may include some degree of required reporting from the	Teams and coordinating teams frequently share tactical, technical information as well as information regarding threats, vulnerabilities, and risks to the community served by the coordinating team. The coordinating team may also need

	member organizations by the coordinating body, as well as the expectation that the coordinating team will disseminate timely and useful information to participating member organizations.	specific impact information about incidents in order to help make decisions on where to focus its resources and attention.
Coordinating team-to coordinating team	Relationships between multiple coordinating teams to share information relating to cross-cutting incidents which may affect multiple communities. The coordinating teams act on behalf of their respective community member organizations to share information on the nature and scope of cross-cutting incidents and reusable mitigation strategies to assist in inter-community response.	The type of information shared by coordinating teams with their counterparts often consists of periodical summaries during "steady state" operations, punctuated by the exchange of tactical, technical details, response plans, and impact or risk assessment information during coordinated incident response activities.