CST
هيئة الاتصالات والفضاء والتقنية
Communications, Space & Technology Commission

Regulations for Cybersecurity Operations in ICT Sector

RT13

Second Version

October 2023

Disclaimer: English language text is not an official translation and is provided for information purposes only. It confers no right and imposes no obligation separate from those conferred or imposed by the original Arabic text formally adopted and published. In the event of any discrepancies between the English translation and the Arabic original, the Arabic original shall prevail.

www.cst.gov.sa

Version Control Table

Version	Issuing Date
Regulations for Cybersecurity Operations in ICT and Postal Sector RT13 First Version	August 2022
Regulations for Cybersecurity Operations in ICT Sector RT13 Second Version	October 2023

TABLE OF CONTENTS

1. Introduction

In accordance with the Communications and Information Technology Act issued by Royal Decree No. (M/106) dated 02/11/1443 AH, and it's Bylaw, and based on the regulatory tasks assigned to CST under its Ordinance, including those related to protecting public interest, user interests, providing protection against harmful content, and preserving the confidentiality of communications; CST issues this document with the aim of enhancing mutual cooperation among service providers in the Information and Communications Technology Sector, and support preparedness and resilience against cyber attacks in the sector.

2. Definitions

The terms and expressions defined in the Communications and Information Technology Act, its Bylaws and other CST statutes shall have the same meanings when used in this document. Furthermore, the following terms and expressions shall have the meanings assigned below unless the context requires otherwise:

Term/Expression	Definition
2.1 CST	Communications, Space and Technology Commission.
2.2 ICT-CSIRT /Center	CST's Cybersecurity Operations Center.
2.3 Service Providers	The providers of telecommunications or information technology services in the ICT Sector within the Kingdom of Saudi Arabia.
2.4 Cybersecurity	Protection of networks, systems, operations, and their components of hardware and software, provided services, and contained data from any unauthorized access or disruption or misuse. The Cybersecurity concept includes information and digital security.
2.5 Cybersecurity Incident	A compromise through violation of cybersecurity policies, acceptable use policies, practices or cybersecurity controls or requirements.
2.6 Vulnerability	Any type of weakness in a computer system, software, application, set of procedures, or in anything that leaves cybersecurity exposed to a threat.
2.7 Cybersecurity Threat	Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. Also, the potential for a threat-source to successfully exploit a particular information system vulnerability.
2.8 Incident Response	Handling an incident through a systematic process that aims at minimizing the incident's impact to the lowest level possible, while specifying and sharing indicators of compromise and detailed digital evidence, along with preparing and submitting the incident-related reports and recommendations.
2.9 Threat Intelligence	It provides organized information and analysis of recent, current and potential attacks that could pose a cyber-threat to the organization.
2.10 Indicators of Compromise	Pieces of forensic data found in files or systems that can enable cybersecurity professionals to detect malicious activity on networks or information technology systems.
2.11 Attack	Any kind of malicious activity that attempts to achieve unauthorized access, collection, disabling, prevention, destruction, or sabotage of information system resources or information itself.

2.12 Indicators of Attack	Traces of instances and actions that an attacker attempted in order to gain unauthorized access to a system or a network before reaching the ultimate goal of abusing vulnerabilities, data theft, or other forms of cyber-attacks.
2.13 Vulnerability Scan	A scan to detect weakness in a computer operating system, software, applications, procedures or any related components that would make cybersecurity vulnerable.
2.14 Threat Hypothesis	A scenario based on the analysis of threat actors or campaigns that can assist in discovering similar Indicators of Attack or Indicators of Compromise in an environment.
2.15 Threat Hunting	A scan based on the Threat Hypothesis to detect Indicators of Compromise in systems or networks.
2.16 Incident Alert	An urgent notice that a specific attack has been directed against an entity's environment.
2.17 Responding Entity	The professional Service Provider that is providing the cybersecurity incidents response service (3rd party).
2.18 Personally Identifiable Information	Information which can be used to distinguish or trace the identity of an individual (e.g. name, biometric records) alone, or when combined with other personal or identifying information which is linked or linkable to specific individual (e.g. date and place of birth).
2.19 Data Leakage	Disclosure, acquisition or access to data without a permit or legal documentation, whether intentionally or unintentionally.
2.20 Personal Data Leakage	Disclosure, publication, acquisition, or access to personal data without a permit or legal documentation, whether intentionally or unintentionally.
2.21 Critical Incident	A Nation-wide or Sector-wide incident of high impact.
2.22 Initial Assessment of Cybersecurity Incident	A brief analysis of the incident with the aim of confirming the validity of incident, specifying its type and classification, collecting initial indicators of compromise and initial determination of the impact of such incident.

3. Scope of Application

This Regulation specifies the roles and responsibilities of ICT-CSIRT and all the Service Providers in the Information and Communications Technology Sector in the Kingdom.

3.1 Compliance with the Regulation

3.1.1 This Regulation applies to all the Service Providers in the Information and Communications Technology Sector in the Kingdom.

3.1.2 The Service Providers shall abide by all procedures contained within the regulation and annexes. Any violation of the subsequent articles shall be dealt with as per CST Regulations. The Service Provider shall not be relieved of liability if contracted with third parties.

3.1.3 This Regulation does not exempt the Service Provider from abiding by any policies or procedures included in any statutory document issued by CST or other relevant entities.

4. General Provisions

4.1 This Regulation does not exempt the Service Provider under any circumstance from their cybersecurity responsibilities, they must take all necessary measures to protect their assets, verifying periodically its readiness to prevent cybersecurity incidents and responding to the incidents, if any.

4.2 The Service Providers shall register with CST and specify the contact details by filling out the form in Annex (A - CST Registration Form) or any other method CST might specify, and such details shall be updated if any change or modification is to be made.
4.3 If necessary, CST may review or update the articles of this Regulation periodically.

5. Cybersecurity Information Sharing

This Article is to organize the mechanism for the exchange of cybersecurity information between ICT-CSIRT and the Service Providers in the ICT Sector. It defines roles and responsibilities that enable ICT-CSIRT to carry out its duties in discovering any targeted cybersecurity campaigns and overseeing the response to cybersecurity threats and incidents, and to promote the Service Providers' readiness against such threats and incidents.

5.1 Roles and Responsibilities

Responsible	Roles & Responsibilities
Service Providers	5.1.1 The Service Provider shall share any cybersecurity-related information with ICT-CSIRT as per periods specified by ICT-CSIRT or upon request, using means provided by the center. Such information shall include at least the following: (a) Initial report of current cybersecurity incidents. (b) Reports on system vulnerabilities. (c) Threat intelligence. (d) Indicators of compromise or attack. (e) Results of cyber exercises. (f) Any other information requested by ICT-CSIRT. 5.1.2 The Service Provider shall share any information on sector-wide cybersecurity threats and incidents upon availability and without ICT-CSIRT request. Any delay or failure to share the collected information is a violation of this Article.
ICT-CSIRT	5.1.3 ICT-CSIRT shall analyze and study the information received. ICT-CSIRT has the right, at its absolute discretion, to share all or part of received information with the relevant entities to protect the public interest and interests of users while maintaining the privacy and confidentiality of such information.

6. Cybersecurity Threat Intelligence Sharing

This Article is to regulate the exchange between ICT-CSIRT and the Service Providers in regard to cybersecurity threat intelligence sharing and define roles and responsibilities. Enabling the threat intelligence sharing service in ICT-CSIRT to provide intelligence on active cybersecurity threats that target the sector; to promote readiness of the Service Providers for responding to cybersecurity threats and raise awareness of cybersecurity threats in the Sector.

6.1 Roles and Responsibilities

Responsible	Roles & Responsibilities
ICT-CSIRT	6.1.1 ICT-CSIRT shall share threat intelligence obtained from the Service Providers in the ICT Sector or other entities, with relevant service providers and entities within the Kingdom. The information shared shall be analyzed, revised and classified. 6.1.2 ICT-CSIRT shall share periodic reports with the Service Providers in the Sector and related entities within the Kingdom 6.1.3 ICT-CSIRT shall maintain the privacy and confidentiality of information received from the Service Providers. ICT-CSIRT may share all or part of the information with the relevant entities to protect the public as well as user interest, while maintaining the privacy and confidentiality of such information.

Service Providers	6.1.4 The Service Provider shall share threat intelligence obtained via its internal networks or by any other source of threat intelligence after they evaluate and verify that such information may have an impact on the other Service Providers. 6.1.5 The Service Provider, via means specified by ICT-CSIRT, shall share any information with ICT-CSIRT proactively, without ICT-CSIRT request, and within the durations specified in the "Level of Compliance Table" below. Any delay or failure to share information shall be deemed a violation of this Article. 6.1.6 All the Service Providers shall implement the necessary mechanisms and techniques to receive or send threat intelligence to ICT-CSIRT. 6.1.7 If a response is requested, the Service Provider shall provide any information related to the threat intelligence previously shared by ICT-CSIRT via means specified by ICT-CSIRT and within the duration specified in the "Level of Compliance Table" below. 6.1.8 The Service Provider shall take all necessary measures to respond to risks and threats shared by ICT-CSIRT.

6.2 Level of Compliance Table

Durations required to implement the activities related to Cybersecurity Threat Intelligence Sharing.

Entity	Durations required to provide any available information related to threat intelligence shared by ICT-CSIRT according to the classifications below				
	Top Priority	High	Medium	Low	No Response Required
Service Providers	One Business Day	3 Business Days	5 Business Days	10 Business Days	-

7. Vulnerability Monitoring & Assessment

This Article aims to regulate the exchange between ICT-CSIRT and the Service Providers in regard to vulnerability scanning, disclosure, and evaluation to enable ICT-CSIRT to carry out its duties by enhancing the capabilities of the Service Providers in managing, monitoring, and addressing vulnerabilities, and reducing the attack surface of the sector.

7.1 Roles and Responsibilities

A. Follow-up and Remediation of Critical Vulnerabilities

Responsible	Roles & Responsibilities
Service Providers	7.1.1 The Service Provider shall provide ICT-CSIRT with all information regarding critical/high-risk vulnerabilities once detected according to the means determined by the Center and periods specified in the "Level of Compliance Table" below. 7.1.2 The Service Provider shall provide ICT-CSIRT with reports on plans to address critical/high-risk vulnerabilities periodically or upon request.
ICT-CSIRT	7.1.3 ICT-CSIRT shall process and analyze information received from the Service Providers on critical/high-risk vulnerabilities. ICT-CSIRT shall provide (if necessary) recommendations and corrective measures that help address or alleviate the impact of such vulnerabilities.

B. Sector-Wide Vulnerability Scan

Responsible	Roles & Responsibilities

ICT-CSIRT	7.1.4 In coordination with the Service Providers, ICT-CSIRT shall determine the scope and timeline of the Vulnerability Scan and share it with the Service Providers before carrying out such scans. 7.1.5 ICT-CSIRT shall carry out a Vulnerability Scan on external web URLs of the Service Providers' networks and systems as per the specified scope and timeline. Furthermore, ICT-CSIRT shall analyze the results of the scan and share the outcome with the Service Provider involved.
Service Providers	7.1.6 The Service Provider shall review the scope and timeline of the scan and provide suggestions and feedback to ICT-CSIRT as per the means determined by ICT-CSIRT and periods specified in the "Level of Compliance Table" below. 7.1.7 Upon receipt of the scan results, the Service Provider must develop a plan to address the discovered vulnerabilities, and then provide ICT-CSIRT with such plan according to the means determined by ICT-CSIRT and periods specified in the "Level of Compliance Table" below.

7.2 Level of Compliance Table

- Durations required to implement the activities related to the follow-up and remediation of critical vulnerabilities.

Entity	Duration for sharing vulnerabilities & remediation plan	Duration for responding to the Service Provider to provide additional recommendations and corrective measures to remediate critical vulnerabilities*	Duration for responding to the Service Provider to provide additional recommendations and corrective measures to remediate high-risk vulnerabilities*
ICT-CSIRT	-	3 Business Days	5 Business Days
Service Providers	4 Business Days	-	-

*Depending on ICT-CSIRT assessment of a vulnerability and the urgency of a response.

- Durations required to implement the activities related to implementing a sector-wide vulnerability scan.

Entity	Duration for feedback on a vulnerability scan scope	Duration for sharing critical vulnerabilities	Duration for sharing high and medium-risk vulnerabilities
ICT-CSIRT	-	2 Business Days	5 Business Days
Service Providers	2 Weeks	-	-

8. Cyber Threat Hunting

This Article is to regulate the exchange between ICT-CSIRT and the Service Providers in regard to Cyber Threat Hunting. Accordingly, ICT-CSIRT will develop hypotheses that contribute to proactively detecting and hunting threats, sharing them with the Service Providers in order to search for indicators of compromise that have not been detected by normal monitoring and detection tools (e.g. anti-virus and anti-malware), and then respond to the detected cyber threats and incidents. The Service Provider can request for a Cyber Threat Hunting exercise from ICT-CSIRT and as such the center will evaluate the request and send the response accordingly. This Article is associated with Article No. 6 **"Cybersecurity Threat Intelligence Sharing".**

8.1 Roles and Responsibilities

Responsible	Roles & Responsibilities
ICT-CSIRT	8.1.1. ICT-CSIRT shall develop and share threat hypotheses based on threat intelligence and cyber incidents of the sector. Such hypotheses shall

	include the guidelines required for threat hunting by the Service Providers. 8.1.2. ICT-CSIRT shall share with the Service Providers, the recommendations drawn from the threat hunting activities after analyzing the results.
Service Providers	8.1.3. The Service Provider shall conduct threat hunting based on the hypotheses provided by ICT-CSIRT, and share the threat hunting results with ICT-CSIRT via means determined by ICT-CSIRT and within the durations specified in the "Level of Compliance Table" below. 8.1.4. The Service Provider shall implement the recommendations and required procedures received from ICT-CSIRT on the threat hunting results. 8.1.5. The Service Provider shall share the information on cyber incidents detected during threat hunting within the durations specified in the "Level of Compliance Table" below, and shall then follow the procedures for responding to cybersecurity incidents, which are included in Article No. 9 **"Handling Cybersecurity Incidents"** of this Regulation.

8.2 Level of Compliance Table

- Durations required to implement the activities related to cyber threat hunting.

Entity	Duration for threat hunting & result sharing	Duration for sharing information on incidents confirmed based on threat hunting
Service Providers	2 Weeks	Immediate

9. Handling Cybersecurity Incidents

This Article is to assign the roles and responsibilities of the relevant entities when responding to cybersecurity incidents. As well as, to ensure the application of measures required to prevent and respond to security risks and incidents in the ICT Sector.

9.1 Roles and Responsibilities

Responsible	Roles & Responsibilities
Service Providers	9.1.1. The Service Provider shall begin the incident response plan procedures upon the incident discovery, and inform ICT-CSIRT immediately via CST Communication Channels defined in Annex (B - CST Communication Channels for Clarification Response) or any other method CST might specify. Then, the Service Provider shall provide all sufficient and related information on the incident to ICT-CSIRT by filling out the Incident Reporting Form in Annex (A - Cybersecurity Incident Reporting Form). 9.1.2. The Service Provider shall assign a liaison officer to answer ICT-CSIRT inquiries and provide ICT-CSIRT with all the required information, if needed, throughout the duration of handling the cybersecurity incidents. 9.1.3. The Service Provider shall conduct the initial assessment of the cybersecurity incident and provide ICT-CSIRT with the results. CST may

	request the Service Provider to re-conduct the initial assessment of the cybersecurity incident in the event of insufficient information, and to analyze the risks arising from the incident. 9.1.4. The Service Provider shall provide ICT-CSIRT with periodic status reports on the current incident via means specified by the Center and according to the "Level of Compliance Table" below. 9.1.5. The Service Provider shall submit, to ICT-CSIRT, a final report on the incident as per report template in Annex (A - Final Report on the Cybersecurity Incident Form) within the duration specified in the "Level of Compliance Table" below. 9.1.6. The Service Provider shall commit to the corrective measures received from ICT-CSIRT within the duration specified in the report. 9.1.7. The Service Provider shall be allowed, with regard to a cybersecurity incident, to communicate with the relevant entities only. 9.1.8. The Service Provider shall, in the event that CST assigns a Responding Entity, fully cooperate and facilitate the work and tasks of CST and the designated Responding Entity, including providing access to the cybersecurity incident site and providing the information and reports required. 9.1.9. The Service Provider shall issue a statement of clarification, at their own expense, on the cybersecurity incident, if needed, upon CST direction. 9.1.10. If the incident would affect other entities, such as the Service Provider's clients, the Service Provider shall send a notification and provide, if needed, a briefing on the incident to the relevant entities and ICT-CSIRT.
ICT-CSIRT	9.1.11 ICT-CSIRT may re-evaluate the cybersecurity incident and classify it as a critical incident, which shall be handled as follows: 9.1.11.1 CST may assign a Responding Entity to cybersecurity incidents and notify the Service Provider. 9.1.11.2 ICT-CSIRT shall assign an internal team to follow up on the incident and coordinate the Service Provider-Responding Entity communication. 9.1.12 ICT-CSIRT may share, at its absolute discretion, the results of the initial, complete or part of final reports prepared by the Service Provider, with the relevant entities, while maintaining the privacy and confidentiality of the information contained within the reports. 9.1.13 ICT-CSIRT may inspect and investigate the cybersecurity incident site, in accordance with CST regulations. 9.1.14 In case of a cybersecurity incident, ICT-CSIRT may request corrective actions to be implemented by the Service Provider in a specified period. 9.1.15 ICT-CSIRT may share, at its absolute discretion, the lessons learned from the cybersecurity incident with other entities inside or outside the sector, while preserving the privacy and confidentiality of the Service Provider. 9.1.16 CST may issue, at its absolute discretion, a statement of clarification on the cybersecurity incident.
Responding Entity	9.1.17 The Responding Entity shall communicate with the Service Provider, request the required information, visit incident site, provide ICT-CSIRT and the Service Provider with periodic reports during the duration of

	handling the cybersecurity incidents, and submit a final report as indicated in the Annex (A - Final Report on the Cybersecurity Incident Form). 9.1.18 The Responding Entity shall provide ICT-CSIRT and the Service Provider with periodic reports during the response service and a final report on the incident, as in Annex (A - Final Report on the Cybersecurity Incident Form).

9.2 Level of Compliance Table

- Durations required to implement the activities related to handling cybersecurity incidents.

Entity	Duration required to inform ICT-CSIRT of the cyber incident	Duration required for sharing periodic status reports	Durations required for submitting Final Report on the Cybersecurity Incident
Service Providers	Immediate	Every 5 Business Days, at least	20 Business Days

10. Cybersecurity Incident Clarification

This Article is to regulate the exchange of cyber information between ICT-CSIRT and the Service Providers, to define roles and responsibilities that enable ICT-CSIRT to carry out its duties to supervise the activities of the Service Providers in responding to cyber threats and incidents, as well as, to assist the Service Providers in preparing to respond to such threats and incidents.

10.1 Roles and Responsibilities

Responsible	Roles & Responsibilities
ICT-CSIRT	10.1.1 ICT-CSIRT shall send a Cybersecurity Incident Clarification request to the point of contact assigned by the Service Provider via the email registered with ICT-CSIRT or to any other communication channel predetermined by the Center. 10.1.2 ICT-CSIRT shall determine, at its absolute discretion, the duration required to respond to the request. 10.1.3 ICT-CSIRT may share, at its absolute discretion, the results of the initial reports prepared by the Service Provider with the relevant entities, in order to safeguard the public and user interests while maintaining information privacy and confidentiality.
Service Providers	10.1.4 The Service Provider shall submit the clarification form as indicated in Annex (A - Cybersecurity Incident Clarification Form) to ICT-CSIRT through the same CST communication channel in Annex (B - CST Communication Channels for Clarification Response). 10.1.5 The Service Provider shall submit the clarification form within the duration specified in the form. If duration extension is needed, the Service Provider shall inform ICT-CSIRT, stating justifications for approval. 10.1.6 The Service Provider shall, if a cybersecurity incident is confirmed, follow the procedures for responding to cybersecurity incidents, which are included in Article No. 9 "Handling Cybersecurity Incidents" of this Regulation.

Annexes

Annex (A): CST Forms

CST Forms include the following:

- CST Registration Form
- Cybersecurity Incident Clarification Form
- Cybersecurity Incident Reporting Form (This form represents the minimum information required during the incident reporting process)
- Final Report on the Cybersecurity Incident Form

Notes:

- All entities shall classify these forms, after filling out, as restricted /confidential information.
- Forms can be downloaded through CST website via the following link: https://www.cst.gov.sa/cybersecurity

Annex (B): CST Communication Channels for Clarification Response

If CST requests a clarification from one of the relevant entities involved, this entity shall immediately follow the above-mentioned procedures and fill out a Cybersecurity Incident Clarification form, Annex (A).

The form in Annex (A) shall be filled out and submitted to the e-mail in the table below or any communication channels that ICT-CSIRT may specify later:

CST Communication Channels	
E-mail	**incident@cst.gov.sa**
Phone No.	**011-461-9999**

هيئة الاتصالات والفضاء والتقنية
Communications, Space &
Technology Commission