Consultative Document

Guidelines for Cybersecurity of Public Telecommunications Networks and Broadcasting Facilities

(Second of Two Rounds)

May 2025 TATT Ref: 2/3/68

Maintenance History		
Date	**Change Details**	**Version**
29th October 2024	First consultative document	0.1
21st May 2025	Second consultative document	0.2

This document may be cited as*:* Telecommunications Authority of Trinidad and Tobago (TATT 2025) *Consultative Document on the Guidelines for Cybersecurity of Public Telecommunications Networks and Broadcasting Facilities* (May 2025). Barataria, Trinidad and Tobago.

Table of Contents

Abbreviations

AES	advanced encryption standard
CBTT	Central Bank of Trinidad and Tobago
CSTAC	Canadian Security Telecommunications Advisory Committee
DNS	domain name service
DNSSEC	domain name service security extension
DOS	denial of service
EBU	European Broadcasting Union
ENISA	European Union Agency for Cybersecurity
GORTT	Government of the Republic of Trinidad and Tobago
GSMA	Global System for Mobile Communications Association
ICT	information and communications technology
IEC	International Electrotechnical Commission
ISMS	information security management system
ISO	International Organization for Standardization
ISP	Internet service provider
IOT	Internet of Things
ITU	International Telecommunication Union
NAB	National Association of Broadcasters
NCSC	National Cyber Security Centre
NIST	National Institute of Standards and Technology
OAS	Organization of American States
RPKI	Resource Public Key Infrastructure
SIEM	security information and event management
SBC	session border controller
SIP	Session Initiation Protocol
SMS	short messaging service
TSP	telecommunications service provider
TT-CSIRT	Trinidad and Tobago Cyber Security Incident Response Team
WPA	Wi-Fi Protected Access
WPA2	Wi-Fi Protected Access version 2
WPA3	Wi-Fi Protected Access version 3

1. Introduction

1.1 Background

Public telecommunications networks and broadcasting facilities form critical infrastructure for businesses, governments, and individuals. These networks provide a wide range of services, including voice, data, and video communications, as well as access to the Internet. As such, they are a prime target for cyberattacks.

In 2012, Trinidad and Tobago developed its *National Cyber Security Strategy* which seeks to guide all initiatives related to cybersecurity. As the *National Digital Transformation Strategy 2024–2027* envisions the universal adoption of information and communications technologies (ICTs), the underlying networks need to be secure. Under the Telecommunications Act, Chap. 47:31 (the Act), the Telecommunications Authority of Trinidad and Tobago (the Authority) is mandated to protect consumers of public telecommunications networks and services, and broadcasting services. Security guidelines can be established to help operators protect public telecommunications networks from unauthorised access, misuse and theft and, in so doing, protect consumers who use these networks and their data.

The Authority recognises the importance of cybersecurity guidelines to ensure the protection of consumers. The scope of such guidelines should include but not necessarily be limited to:

1. Network architecture and design: The network architecture should be designed to minimise security risks. For example, networks should be segmented to isolate critical systems from less critical systems.

2. Access control: Access to network resources should be restricted to authorised users only. This can be achieved through a variety of methods, such as passwords, multi-factor authentication, and role-based access control.

3. Security monitoring: Networks should be monitored for suspicious activity. This can be done through a variety of methods, such as intrusion detection systems, security information and event management (SIEM) systems, and log analysis.

4. Incident response: Network operators should have a plan to respond to security incidents, which includes steps to identify, contain, eradicate, and recover from them.

5. Data storage: All critical and user data should be effectively protected with backups.

In light of this recognition and the growing threat of cyberattacks, the Authority has prepared these *Guidelines for Cybersecurity of Public Telecommunications Networks and Broadcasting Facilities* to fulfil in part its mandate of consumer protection.

1.2 Purpose

The purpose of this document is to establish practices that are recommended or must be adopted by the operators of public telecommunications networks and broadcasting facilities in Trinidad and Tobago, to protect consumers and their information from cyberattacks.

1.3 Objectives

This document:

1. describes key cybersecurity policies and frameworks in place in Trinidad and Tobago.

2. identifies relevant regional and global standards and recommendations that are applicable to the telecommunications and broadcasting sectors in Trinidad and Tobago.

3. provides recommended and compulsory guidelines for operators of public telecommunications networks and broadcasting facilities to secure those networks and facilities, to protect their customers and customer information.

1.4 Scope

The guidelines in this document have been developed based on the existing regulatory framework for the telecommunications and broadcasting sectors, to protect the interests of the public. These guidelines apply to public telecommunications networks that are based on Internet Protocol (IP) or provide connectivity to the Internet.

These guidelines do not apply to the security approaches to be adopted by end users, whether individual or business, to protect their networks and/or services. These guidelines also do not address redundancy against material loss of facilities due to natural disasters or similar force majeure events, nor responses to emergencies outside of cybersecurity issues.

1.5 Relevant Legislation

The sections of the Act that inform this document are:

Section 3:

The objects of the Act are to establish conditions for –

c) promoting and protecting the interests of the public by –
(iii) providing for the protection of customers;

Section 18 (1):

Subject to the provisions of this Act, the Authority may exercise such functions and powers as are imposed on it by this Act and in particular –

d) establish national telecommunications industry standards and technical standards

o) test and certify telecommunications equipment, subject to section 48(3), to ensure compliance with—
(i) international standards; and
(ii) environmental health and safety standards, including electromagnetic radiation and emissions;

Section (24)(1):

In addition to the conditions stipulated in section 22, a concession for a public telecommunications network or public telecommunications service shall require the concessionaire to adhere, where applicable, to conditions requiring the concessionaire to –

a) submit to the Authority plans for its approval respecting –
(i) the development of its network or service;
(ii) quality of service; and
(iii) any other related matter as the Authority may require,

j) refrain from using, and maintain the confidentiality of any confidential, personal and proprietary information of any user, other operator of a public telecommunications network or other provider of a telecommunications service originating from–
(i) any such user, operator or provider, or;
(ii) any information regarding usage of the service or information received or obtained in connection with the operation of the concessionaire's network or service,
for any other purpose other than to–

(iii) operate such network or service;
(iv) bill and collect charges;
(v) protect the rights or property of the concessionaire
(vi) protect users or other providers from the fraudulent use of the concessionaire's network or service,

or as otherwise permitted by the concessionaire, user or other provider, as the case may be;

Section 32:

Any terminal equipment may be connected to a public telecommunications network where the Authority, after consultation with the concessionaire, has certified such terminal equipment as –

(a) being safe for the user;

(d) not posing a risk of harm to the network;

Section 45:

(2) Notwithstanding subsection (1), the Authority may identify, adopt or establish preferred technical standards.

Section 47:

(1) To ensure compliance with the conditions of a concession or licence, or for any other purpose authorised pursuant to this Act, an inspector may require a concessionaire or licensee to supply information, including specific answers to questions submitted to such concessionaire or licensee, concerning any telecommunications network or telecommunications or radio-communications service for which the concession was granted or the licence issued, the operation of any equipment or any works carried out in relation to such network or service.

Section (48)(3):

The requirement for testing may be waived by the Authority, after consultation with the concessionaire or licensee, if the Authority is satisfied that the equipment has been certified in accordance with international standards.

1.6 Other Relevant Documentation

Other relevant policies, plans and regulations developed by the Authority, currently in effect, to be read along with this document, include:

1. *Authorisation Framework for the Telecommunications and Broadcasting Sectors of Trinidad and Tobago*

2. *Procedures for Consultation in the Telecommunications and Broadcasting Sectors of Trinidad and Tobago*

3. *Technical Standards for Public Fixed Telecommunications Networks*

4. *Technical Standards for Wireless Networks*

These documents can be found on the Authority's website, www.tatt.org.tt. The technical standards are particularly relevant as they pertain to resiliency of telecommunications networks.

1.7 Review Cycle

This document will typically be reviewed every four years, to ensure it continues to adapt to the needs of the telecommunications and broadcasting industry and meet changing circumstances. It may, however, be reviewed at any time, at the discretion of the Authority, based on proposals for modification submitted by stakeholders or members of the public or changes in international regulations. The Authority will review the document and, if necessary, make modifications, in consultation with stakeholders, to ensure that the guidelines remain informed by appropriate policy.

Questions or concerns regarding the maintenance of this document may be directed to the Authority via email at consultation@tatt.org.tt.

1.8 The Consultation Process

In accordance with its *Procedures for Consultation in the Telecommunications and Broadcasting Sectors of Trinidad and Tobago* (TATT 2021), the Authority sought the views of stakeholders and the public on this document. On 29th October 2024, the document was issued for the first of two rounds of public consultation for a period of four weeks, ending 26th November 2024. The consultation period was extended for a further two weeks, ending 13th December 2024.

The document will undergo a second round of public consultation, which shall be at least four weeks in duration. Comments from this round will be reviewed and those determined to be relevant and useful will be incorporated.

1.9 Definitions

Access control: preventing the unauthorised use of a resource, including the prevention of the use of a resource in an unauthorised manner, or limiting the flow of information from the resources of a system to authorised persons or systems only (ITU 2015)

Broadcasting facilities: facilities that provide broadcasting services as defined in the Act

Critical network infrastructure[1]: the vital networks, devices, systems or data that the incapacity of, destruction of, or interference with would have a debilitating effect on public safety or national security, or the provision of essential services directly related to the communications infrastructure of Trinidad and Tobago

Cyberattack: activities undertaken to bypass or exploit deficiencies in a digital[2] system's security mechanisms. A direct attack on such a system exploits deficiencies in the underlying algorithms, principles, or properties of a security mechanism. Indirect attacks bypass the security mechanism or make the system use the mechanism incorrectly.

Cybersecurity: the collection of tools, policies, actions, systems and processes that can be used to protect the cyber environment and an organisation's assets, and will minimise the vulnerabilities of critical network, system and information assets and resources (ITU 2009) (ITU 2015)

Cyber threat: a potential violation of the security of a network, its assets and its resources (ITU 2015)

Facility: a physical component of a telecommunications network (other than terminal equipment), including wires, lines, terrestrial and submarine cables, wave guides, optical or other equipment or object connected therewith, used for the purpose of telecommunications, and any post, pole, tower, standard, bracket, stay, strut, insulator, pipe, conduit, or similar thing used for carrying, suspending, supporting or protecting the structure (TATT 2004)

Incident: an event having a potential or actual adverse effect on the security of a public telecommunications network (ENISA 2021) or broadcasting facilities, and comprising an attempt to infiltrate, or actual infiltration of, a network element or system, or the degradation or loss of public telecommunications service due to a cyber threat or cyberattack

[1] Definition adapted from the National Cyber Security Strategy (GoRTT 2012) and International Telecommunication Union Background Paper on Cybersecurity (ITU 2009)
[2] Digital inserted in the definition contained within the ITU Report on *Security in Telecommunications and Information Technology* (ITU 2015).

Public telecommunications network: a system or part thereof used to provide a public telecommunications service, which shall include providing a broadcasting service (TATT 2004)

1.10 Conformance Notation

The guidelines in this document are classified as either required or recommended, which for the purpose of these guidelines are defined as follows:

Required	The operator shall comply fully with the guideline as specified.
Recommended	The operator is encouraged to adopt the guidelines as specified. There may exist valid reasons in particular circumstances where the specified guideline cannot be implemented; in such instances, if the operator does not observe the guideline, the full implications of the circumstance must be carefully considered by the operator.

2. The Cybersecurity Framework in Trinidad and Tobago

2.1 National Cybersecurity Policy Overview

In December 2012, an Inter-Ministerial Committee for Cyber Security was appointed, which developed the *National Cyber Security Strategy* for the Government of the Republic of Trinidad and Tobago (GORTT). This strategy is intended to guide all operations and initiatives related to cybersecurity in Trinidad and Tobago and is based on the Government appreciating the role of ICTs in advancing national development (GoRTT 2012). Its main objectives are to:

1. create a secure digital environment that will enable all users to enjoy the full benefits of the Internet.

2. provide a governance framework for all cybersecurity matters, by identifying the requisite organisational and administrative structures, including human resources, training and capacity building and budgetary resources.

3. protect the physical, virtual and intellectual assets of citizens, organisations and the state, through the development of an effective mechanism that addresses and responds to cyber threats regardless of their origin.

4. facilitate the safety of all citizens by promoting awareness of cyber risks and developing effective and appropriate protective measures to mitigate risks and attacks.

5. help prevent cyberattacks on critical infrastructure and secure information networks, by building competency among primary stakeholders and the general public.

6. minimise the damage and recovery times following cyberattacks, through effective incident management measures.

7. create a legal and regulatory framework to maintain order, protect the privacy of users, and criminalise attacks in cyberspace.

2.2 Trinidad and Tobago Cyber Security Incident Response Team (TT-CSIRT)

To advance the strategic objectives of the *National Cyber Security Strategy*, GORTT, through the Ministry of National Security, established the Trinidad and Tobago Cyber Security Incident Response Team (TT-CSIRT) in November 2015, with the assistance of the Organization of American States (OAS) and the International Telecommunication Union (ITU). TT-CSIRT

was established to respond to cyber incidents through effective response techniques, education, training, awareness, research, collaboration and efficient management strategies, to restore the operations of the information systems of its constituents. Its goals are to:

1. develop a framework and related policies and procedures for the coordinated response and management of cyber incidents.

2. facilitate information sharing among the TT-CSIRT constituency relating to best practices, investigative information, coordinating incident response, and incident management procedures and processes.

3. identify critical infrastructure and assess the level of vulnerability to cyber threats.

4. provide technical assistance to GORTT and other stakeholders within the national framework.

5. defend against attacks, with special focus on critical information infrastructure.

6. develop frameworks and guidelines for business continuity readiness assessments and the development of information technology (IT) disaster recovery and business continuity plans.

7. collect data and statistics on cyber incidents.

8. build capabilities for managing cyber threats and enhancing cybersecurity.

TT-CSIRT has identified critical infrastructure as an important target for cybersecurity and protection. As the country embarks on its digital transformation journey, national public telecommunications networks and broadcasting infrastructure form part of the critical infrastructure that must be protected.

2.3 Central Bank of Trinidad and Tobago Cyber Security Best Practices Guideline

The Central Bank of Trinidad and Tobago (CBTT) published its *Cyber Security Best Practices Guideline* in September 2023, to provide its licensees and related companies with guiding principles that are consistent with best practices that can be leveraged to enhance their cyber resilience (CBTT 2023). The requirements to be adopted are proportional to the company's business model, complexity of operations, and risks. CBTT's guideline accords with the Financial Institutions Act and the Insurance Act. It should be read in conjunction with CBTT's *Guideline on Security Systems for Safeguarding Customer Information* (2015) and its *Guideline for the Management of Outsourcing Risks* (2022). Institutions not regulated by

CBTT are encouraged to adopt the provisions in CBTT's guideline to manage their cyber risks but are not required to report to CBTT.

CBTT authorises several entities that are or whose affiliates are authorised by the Authority. This is not unique to Trinidad and Tobago, where operators of public telecommunications networks provide digital financial services such as digital wallets, fund transfers and electronic payments. It is therefore useful for the guidelines established by the CBTT and the Authority to be aligned as far as reasonably possible.

2.4 Data Protection Legislation

In 2011, Trinidad and Tobago enacted its Data Protection Act (MAGLA 2011), the objective of which is to ensure that protection is afforded to individuals' right to privacy and the right to maintain sensitive personal information as private and personal. The Act outlines the General Privacy Principles which are applicable to all persons or entities that handle, store or process personal information belonging to another person, which are:

1. An organisation shall be responsible for the personal information under its control.

2. The purpose for which personal information is collected shall be identified by the organisation before or at the time of collection.

3. Knowledge and consent of the individual are required for the collection, use or disclosure of personal information.

4. The collection of personal information shall be undertaken and be limited to what is necessary, in accordance with the purpose identified by the organisation.

5. Personal information shall only be retained for as long as is necessary for the purpose collected and shall not be disclosed for other purposes without the prior consent of the individual.

6. Personal information shall be accurate, complete and up to date as is necessary for the purpose of collection.

7. Personal information is to be protected by appropriate safeguards having regard to the sensitivity of the information.

8. Sensitive personal information is protected from processing except where otherwise provided for by written law.

9. Organisations are to make available to individuals documents regarding their policies and practices related to the management of personal information except where otherwise provided by written law.

10. Organisations shall disclose at the request of the individual, except where otherwise provided by written law, all documents relating to the existence, use and disclosure of personal information, such that the individual can challenge the accuracy and completeness of the information.

11. The individual can challenge the organisation's compliance with these principles and receive timely and appropriate engagement from the organisation.

12. Personal information that is requested to be disclosed outside of Trinidad and Tobago shall be regulated and comparable safeguards to those under this Act shall exist in the jurisdiction receiving the personal information.

It should be noted that Part I, which prescribes the General Privacy Principles, sections 7 to 18, 22, 23, 25(1), 26 and 28 of Part II, and 42 (a) and (b) of Part III of the Data Protection Act have been proclaimed at this time[3]. Therefore, the General Privacy Principles are fully in effect.

[3] Law in Trinidad and Tobago - DLA Piper Global Data Protection Laws of the World (dlapiperdataprotection.com)

3. Relevant Global Cybersecurity Standards and Guidelines

The Authority has identified various global standards and best practice guidelines established by recognised agencies such as the Canadian Security Telecommunications Advisory Committee (CSTAC), the European Broadcasting Union (EBU), the European Union Agency for Cybersecurity (ENISA), the International Organization for Standardization (ISO), the International Electrotechnical Commission (IEC), ITU, the National Association of Broadcasters (NAB) and the National Institute of Standards and Technology (NIST).

3.1 Security Best Practices for Canadian Telecommunications Service Providers

The best practices defined in this document prepared by CSTAC are designed to give guidance to telecommunications service providers (TSPs) on how best to secure their networks (CSTAC 2013). The practices defined within are intended as voluntary, and they ensure that TSPs have a common understanding of what is a secure, resilient, available communications service, and how it should be managed. The best practices identify the controls that any service provider should have in order to detect cyber threats, thereby helping the service provider protect both its customers' interests and its own infrastructure.

3.2 ITU Security in Telecommunications and Information Technology Manual

This manual provides an overview of telecommunications and information technology security, examines some of the associated practical issues, and indicates how different aspects of ICT security are being addressed by the Telecommunication Standardization Sector of ITU (ITU-T) (ITU 2015). The manual provides tutorial material as well as links to more detailed guidance and additional reference material. In particular, it provides direct links to ITU-T Recommendations and relevant outreach documents. It brings together selected security-related material from ITU-T Recommendations and explains the relationship between various aspects of the work. The results achieved in ITU-T security-related standardisation are also included.

3.3 ISO/IEC 27001 Information Security, Cybersecurity and Privacy Protection

ISO/IEC 27001 is the best-known international standard for information security management systems (ISMSs) and defines the requirements ISMSs must meet (ISO/IEC 2022). The standard provides companies of any size and from all sectors with guidance for establishing, implementing, maintaining and continually improving ISMSs. An organisation or business that conforms with ISO/IEC 27001 has put in place a system to manage risks related to the security of data owned or handled by the company and ensures that this system respects all the best practices and principles enshrined in the standard. While ISO/IEC 27001 outlines the

requirements for an ISMS, ISO/IEC 27002 offers control objectives related to cybersecurity aspects of an ISMS.

3.4 ITU-T Recommendation X.1051 – Information security controls for telecommunications organisations

ITU-T Recommendation X.1051 – Information security controls based on ISO/IEC 27002 for telecommunications organisations, is also referred to as the standard ISO/IEC 27011 (ITU 2023). It establishes guidelines and general principles for initiating, implementing, maintaining and improving information security controls in telecommunications organisations, based on ISO/IEC 27002, and provides an implementation baseline of information security controls within telecommunications organisations, to ensure the confidentiality, integrity and availability of telecommunications facilities, services and information handled, processed or stored by the facilities and services.

3.5 ENISA Guidelines on Security Measures

This document, the ENISA Guidelines on Security Measures under the European Electronic Communications Code (EECC) (ENISA 2021), prepared by the European Union Agency for Cybersecurity (ENISA), provides technical guidance to competent national authorities about how to ensure technically that providers assess risks and take appropriate security measures.

3.6 The NIST Cybersecurity Framework (CSF) 2.0

This framework, published by the National Institute of Standards and Technology (NIST) in the United States, is a guide for identifying and describing an organisation's current and target cybersecurity posture, based on a detailed taxonomy of high-level cybersecurity outcomes (NIST 2024). These outcomes can be understood by a broad audience, regardless of their cybersecurity expertise. The CSF aids in identifying the outcomes for addressing the unique cybersecurity risks of a specific organisation. It does not describe how these outcomes can be achieved but provides links to online resources accessible through the NIST CSF website.

3.7 The Essential Guide to Broadcasting Cyber Security

This report, published in 2016 by the National Association of Broadcasters (NAB) for the United States, presents an overview of key resources that can be used to minimise the risk of a cyberattack and prevent major losses (NAB 2016). It discusses three main resources, the first of which is the NIST *Framework for Improving Critical Infrastructure Cybersecurity*. The second document is the Communications Security, Reliability and Interoperability Council (CSRIC) *Cybersecurity Risk Management and Best Practices* – Working Group 4 Final Report, issued by CSRIC working under the Federal Communications Commission (FCC). The final resource is the Initial Report by the CSRIC WG3 Emergency Alert System (EAS) Security

Subcommittee. This report includes a section that lists the 35 cybersecurity activities from the NIST Framework that were identified by the CSRIC WG4 broadcast subgroup to be critical for every type of broadcaster.

3.8 Cybersecurity Recommendation R 143 v2.4 for Media Vendors' Systems, Software & Services

Cybersecurity Recommendation R 143 v2.4 for Media Vendors' Systems, Software & Services, was published by the European Broadcasting Union (EBU) in March 2016 and contains a security controls assertation spreadsheet that functions as a checklist for media vendors, to help identify their capabilities for responding to security safeguards during a tendering process (EBU 2024). This checklist is designed as the basis for setting minimal system acceptance levels. The associated documentation provides guidance on how to complete each Excel worksheet that makes up the checklist, with Annex A corresponding to elements related to the vendor's security management system; Annex B corresponding to the vendor's platform if it is a media appliance; and Annex C corresponding to hosted platforms that are delivered as software as a service (SaaS).

3.9 GSMA Baseline Security Controls

This document outlines a specific set of security controls that the mobile telecommunications industry should consider adopting (GSMA 2024). The solution description identifies specific recommendations that would allow operators to fulfil the control objectives. These controls are not binding and represent a voluntary scheme to enable an operator to assess and understand their own security controls. GSMA also develops and maintains the Network Equipment Security Assessment Scheme (NESAS) which provides a universal industry standard that acts as a security baseline against which vendors and their equipment can be tested and audited (NESAS 2023).

These standards and recommendations, and references therein, have been used by the Authority in formulating its guidelines for the adoption of cybersecurity practices within the telecommunications and broadcasting sectors.

4. Guidelines for Cybersecurity of Public Telecommunications Networks and Broadcasting Facilities

The Authority, as the regulator of the telecommunications and broadcasting sectors, will encourage the adoption of best practices by the operators of public telecommunications networks and broadcasting facilities, to secure users of public telecommunications and broadcasting services. Suitable timeframes will be established for the adoption of these guidelines by operators and service providers in the two sectors.

Considering the established global standards and recommendations, the Authority urges operators of public telecommunications networks and broadcasting facilities to adopt the ISO 27001 standard on information security management system requirements, under the controls specified in ITU-T Recommendation X.1051, also referred to as ISO/IEC 27011, to protect critical network infrastructure.

Guideline for Cybersecurity of Public Telecommunications Networks and Broadcasting Facilities (Recommended) – Adoption of ISO 27001

1. *Operators of public telecommunications networks and broadcasting facilities are urged to adopt the ISO 27001 standard on information security management system requirements under the controls specified in ITU-T Recommendation X.1051, to protect their critical network infrastructure.*

In keeping with the objectives of the *National Cyber Security Strategy* and TT-CSIRT, the Authority will address the following specific areas through these guidelines for cybersecurity of public telecommunications networks and broadcasting facilities:

1. Protection of critical network infrastructure
2. Network security monitoring and detection
3. Responsible use and delivery of messaging services
4. User and network interconnection
5. Incident response capability and preparation
6. Development and maintenance of cybersecurity plans
7. Incident reporting
8. Supply chain and vendor management
9. Subscriber privacy and data protection
10. Cybersecurity awareness and education for staff and customers

4.1 Protection of Critical Network Infrastructure

Critical network infrastructure refers to the vital networks, devices, systems or data that the incapacity of, destruction of, or interference with would have a debilitating effect on public safety or national security, or the provision of essential services directly related to the communications infrastructure of Trinidad and Tobago. Public telecommunications networks comprise critical infrastructure elements that are responsible for various functions. These functions involve the carriage of network traffic and include management functions such as remote access; configuration backup; control functions; routing; and traffic shaping. Signalling is necessary to enable communications functions, such as connection establishment and routing determination in public telecommunications networks, including those that provide broadcasting services, and is carried using control channels. Operators should further implement mechanisms to protect the control channels and the signalling traffic itself, whether through encryption, the use of key public infrastructure, or other means.

All of these functions need to be secured to ensure the proper functioning of the networks, and that the data exchanged between users cannot be compromised (Canadian Security Telecommunications Advisory Committee) (CSTAC 2013). Management access should be restricted to end-user computer devices and services, referred to as hosts, which are approved to have such access and should be monitored and logged in all critical systems. Operators should employ mechanisms to secure their signalling traffic, including the routing information generated and exchanged within and among networks.

Critical core network elements are those components that are essential for the functioning of telecommunications networks and therefore must be secured, where the core network refers to the backbone of a telecommunications network that provides services such as authentication and call control to the customers of the network. These elements should be sufficiently maintained to ensure that the most secure versions of operating software are deployed to minimise security vulnerabilities. Operators can also consider adopting zero trust network architectures, which would assume no trust for users or systems inside or outside their networks. This can include the micro-segmentation of their networks to minimise the breadth of potential cyberattacks, and continuous authentication and verification of devices, users and systems.

Guideline for Cybersecurity of Public Telecommunications Networks and Broadcasting Facilities (Recommended) – Protection of Critical Network Infrastructure

2. Operators of public telecommunications networks and broadcasting facilities should possess the capability to:

1) *restrict, monitor and log management access to approved hosts and services.*
2) *log and monitor critical events for network elements.*
3) *implement mechanisms to protect control channels and signalling traffic.*
4) *secure all critical core network elements.*
5) *ensure network elements are maintained at their most secure versions.*

The Domain Name System (DNS) performs an essential translation function in IP networks, from host names to IP addresses, which allows users to establish connectivity to the Internet and access the services they desire. However, the DNS presents a particular possibility for customers' services to be hijacked or compromised. As most contemporary public telecommunications networks use IP for connectivity to the Internet or delivery of their services, the DNS has become an essential control protocol that supports their operation. DNS servers operated by public telecommunications network operators must be secured and provide accurate data (CSTAC 2013).

Guideline for Cybersecurity of Public Telecommunications Networks and Broadcasting Facilities (Recommended) – Protection of Critical Network Infrastructure

3. Operators of public telecommunications networks based on IP should deploy secure and resilient DNS infrastructure and services, according to industry-recognised standards, to protect their own domain and the domains for which they are responsible.

4.2 Network Security Monitoring and Detection

Public telecommunications networks and broadcasting facilities carry different forms of network traffic, such as management, control or data, to support the services they provide. Management traffic is used to ensure the network functions as intended, including monitoring traffic. Control traffic is used to enable the functionalities present in the network, including connection establishment, disconnection, domain name translation, and routing determination, while data traffic refers to the actual traffic being communicated between users of the networks, including voice, video and text. Operators of public telecommunications networks and broadcasting facilities should be able to monitor all network traffic, whether management, control or data, to detect malicious behaviours and activity.

Operators should also be able to analyse cybersecurity logs and monitoring systems to detect anomalous behaviours for further investigation (CSTAC 2013). Volumetric monitoring, which examines the volume of traffic carried on links within the network to establish reasonable baselines for traffic volumes and to identify when traffic volumes do not conform with these baselines, should be employed by operators to ensure abnormal traffic levels are detected and investigated.

Operators should monitor their critical network assets, which are those network elements that are essential to the operation and performance of public telecommunications networks. These must be protected from internal and external threats. Threats are potential harms, that can originate either internally or externally, to public telecommunications networks to compromise their services or performance or the sensitive information they store or generate. Devices and platforms are those components that are connected to the public telecommunications networks to perform any management or control function or provide their services. These can be compromised by potential cyber threats and should therefore be monitored by security information and event management systems, so that any compromise can be detected either before, during or after a cyberattack.

Guidelines for Cybersecurity of Public Telecommunications Networks and Broadcasting Facilities (Recommended) – Network Security Monitoring and Detection

4. *Operators of public telecommunications networks and broadcasting facilities should monitor network traffic to detect malicious behaviour and activity, including through volumetric monitoring.*

5. *Operators should protect critical assets from internal and external threats.*

6. *Operators should maintain security information and event management systems that collect and correlate information from their various devices and platforms.*

Network operators that monitor the nature and trends of traffic on their network can detect traffic anomalies. Identification of these anomalies through signature (based on defined criteria), heuristic (based on similar or resembling attributes) or volume (based on magnitude) characteristics will assist in the detection of malware that may not likely be detected on a device that is compromised, as its own detection mechanisms may be undermined by the malware. It will also assist in the detection of network system abuse, where a critical system such as DNS is inundated with malicious requests such as denial of service (DOS) attacks, which negatively impacts the performance of other customers; sheer brute force means, which include repeated log-in attempts with different credentials; and message abuse, where large volumes of email messages or outbound spam from hosted services provided by the operators may cause blacklisting of IP addresses and domains, or are the source of phishing or other cyberattacks.

Guidelines for Cybersecurity of Public Telecommunications Networks and Broadcasting Facilities (Recommended) – Network Security Monitoring and Detection

7. *Operators should log, monitor and identify the sources of malicious and abnormal traffic, through signature, heuristic, and volume characteristics.*

8. *Operators should monitor and log traffic flows and volumes from internal users and public customers to critical network infrastructure and its services.*

9. *Operators should monitor for, and log the misuse of, email service provision and high volumes of spam-related traffic, emanating from the hosted services provided to their customers.*

4.3 Responsible Use and Delivery of Messaging Services

Messaging services are used widely by subscribers of public mobile communications services, not only to contact other subscribers with personal messages, but also for the dissemination of notifications to customers of other services (such as banking, government, and retail); marketing message delivery by telecommunications and other providers; and even tokens for service authentication as part of a multi-factor authentication process, where customers are notified of an additional verification token after entering their user credentials via an app or website. Messaging services can use many forms of delivery, but typical channels include short messaging service (SMS) and email delivery.

Messaging channels have, however, become a common means by which cyberattacks are pursued, through the use of spamming and phishing messages to deceive unsuspecting subscribers of public telecommunications services. For example, it is typical for large numbers of users to receive an SMS message to transmit funds to an account number or to claim a prize by providing personal information, with the expectation that a small percentage of users would believe the offer is legitimate. Public telecommunications network operators can play a significant role in protecting end users from these attacks.

SMS has also proven to be vulnerable or susceptible to cyberattacks as it is not encrypted. SMS channels should therefore not be used by network operators for the conveyance of persistent user credentials, such as username, account number, personally identifiable information and/or passwords, or sensitive personal financial information, as in credit card or bank account information, to conduct transactions requiring credit card or bank account information, in the delivery of its services, whether related to public telecommunications or other services, such as its financial technology (fintech) solutions. For avoidance of doubt, SMS can be used by operators for the delivery of dynamically generated tokens, as part of a two-factor or multi-factor authentication process. Mechanisms that public telecommunications network operators can pursue include the non-delivery of broadcast SMSs from non-verified sources or networks.

Guidelines for Cybersecurity of Public Telecommunications Networks and Broadcasting Facilities (Recommended) – Responsible Use and Delivery of Messaging Services

10. Public telecommunications network operators should implement suitable mechanisms to mitigate the use of SMS for cyberattacks, including, but not limited to, the mitigation of SMS spamming.

11. Public telecommunications network operators should not use SMS for the transmission of sensitive, persistent user credentials and sensitive personal financial information, such as credit card numbers to enable their customers to access their operator accounts.

4.4 User and Network Interconnection

Connectivity with users and other public telecommunications networks should be secure, as it presents a widely available means of unauthorised access and potential compromise of a public telecommunications network and/or its users. Operators are encouraged to adopt secure protocols to protect the integrity of the connections to their networks. Operators should validate end devices, such as customer premise equipment, that are owned by the operator and that connect to their public telecommunications network. User connectivity should adopt contemporary secure protocols for Wi-Fi access on network customers' premises, such as Wi-Fi Protected Access version 2 (WPA2) with the advanced encryption standard (AES) or version 3 (WPA3) by default. Operators that allow application-based client access to public telephone services using Session Initiation Protocol (SIP), either for business or residential users, are encouraged to use session border controllers (SBCs) (ITU 2015) and strong user and authentication credentials to mitigate the possibility of SIP clients being compromised. Operators should also ensure that customer premise equipment is maintained securely through appropriate patching and upgrades.

To allow users and services of one telecommunications operator to communicate with another, network-to-network interconnection points between the operators are implemented. If unsecured, these interconnection points can allow cyberattacks to either network. It is essential that all partner networks and systems, with which signalling, including routing, and user data traffic are exchanged, are fully validated to keep networks secure. Operators utilising the interconnection points should authenticate the networks to which they are connected and employ appropriate access and filtering mechanisms, so that traffic can only be terminated from authorised network partners, particularly where SIP and Internet-based connectivity are deployed. Resource Public Key Infrastructure (RPKI) is a specialized framework to support improved security for the Internet's routing infrastructure. The use of RPKI, SBCs or similar technology is particularly relevant in these scenarios.

Guideline for Cybersecurity of Public Telecommunications Networks and Broadcasting Facilities (Recommended) – User and Network Interconnection

12. Operators of public telecommunications networks and broadcasting facilities should implement appropriate security measures for user connectivity and network interconnection, to protect end users, their networks and interconnected networks.

4.5 Incident Response Capability and Preparation

Operators of public telecommunications networks and broadcasting facilities must be prepared and able to respond to detected cyberattacks through appropriate incident response procedures, to limit the adverse effects of, and enable recovery from, a network compromise. This may include being able to suspend or disable network access to compromised end users or devices; maintaining copies of critical configuration or user information which can be used to restore service connectivity and information access; limiting, throttling, filtering or blocking certain traffic flows to mitigate any service degradation that may occur; and identifying and notifying the customers impacted of the event occurrence and the estimated timeframe for resolution, and confirming when the matter has been resolved.

Operators must have the capacity to respond to incidents, both internal and external to their networks, and are required to have well-defined, repeatable processes for responding to these events as part of their cybersecurity plans. Operators must be able to respond to security incidents during working and off-hour times, as part of the network security plans to be developed and approved, as required under section 24(1)(a) of the Act.

Guideline for Cybersecurity of Public Telecommunications Networks and Broadcasting Facilities (Required) – Incident Response Capability and Preparation

13. Operators of public telecommunications networks and broadcasting facilities shall be able to respond to threats and attacks they detect through their monitoring programme. Their response shall be well defined and documented and include how the impact of the incident will be contained, how services will be restored, and how customers will be notified.

4.6 Development and Maintenance of Cybersecurity Plans

As part of the preparation to secure their networks and respond to incidents, operators of public telecommunications networks and broadcasting facilities will be required to develop cybersecurity plans. These plans shall detail the specific measures that operators will implement to ensure their networks and corresponding elements are secure; for example, access is restricted to those who require it; critical network infrastructure is hardened and protected as far as reasonably possible; how the security of the network and threats, attacks and compromises will be monitored and logged; how operators will respond to incidents, whether purely at threat stage or if an actual cyberattack has occurred; and how the security of the network will be continually tested and updated.

Under section 24 (1) (a) of the Act, a concessionaire is required to submit to the Authority for approval its plans in relation to its network development, quality of service and any other matter the Authority may require. As cybersecurity preparation involves network development and affects the quality of service provided by network operators, operators will be required by the

Authority to document their plans and procedures relating to the securing of their networks from cyber threats and attacks, either as part of existing network development and quality of service plans, or as a separate and dedicated plan addressing how the network will be developed and maintained, and the quality of service assured in relation to cybersecurity. The cybersecurity procedures should also include those related to the response to cyberattacks and the reporting of the cyberattacks. Where the Authority deems these plans inadequate in relation to network development and quality of service, operators shall revise accordingly to address the concerns identified by the Authority.

These plans shall be developed within one year of these guidelines being effective and operators are directed to do so by the Authority and shall address the main thematic areas as outlined in these guidelines. Plans should also be reviewed at least annually, or when a major threat is identified, to ensure they are relevant to the threat assessment conducted or published by TT-CSIRT and other recognised cybersecurity authorities and resources. In addition to the plans being reviewed, the independent testing of the networks and systems under the plans is also to be conducted, annually, and can include desktop simulations, vulnerability assessments, security penetration testing, governance and access control reviews, and security monitoring and detection audits.

Guidelines for Cybersecurity of Public Telecommunications Networks and Broadcasting Facilities (Required) – Development and Maintenance of Cybersecurity Plans

14. Operators of public telecommunications networks and broadcasting facilities shall prepare and submit to the Authority their cybersecurity plan, or suitable independent certification of its existence, within one year of being directed to do so by the Authority. Where the Authority deems this plan inadequate in areas related to network development and quality of service, operators shall revise their plan accordingly.

15. Operators shall review this plan at least annually, or when a major threat is identified, to ensure it is relevant to the threat assessment of TT-CSIRT or other recognised cybersecurity authority.

Guideline for Cybersecurity of Public Telecommunications Networks and Broadcasting Facilities (Recommended) – Development and Maintenance of Cybersecurity Plans

16. Operators should conduct annual independent testing of their networks and related systems under the plan, which can include simulations, vulnerability assessments, security penetration testing, governance and access control reviews, and security monitoring and detection audits.

4.7 Reporting of Cyber Incidents

Information sharing and reporting are crucial components of protecting critical infrastructure. The extent, breadth, and complexity of contemporary threats require cooperation among operators of public telecommunications networks and broadcasting facilities and other agencies, to protect the critical network and information infrastructure of Trinidad and Tobago.

The Authority understands that, during an event, an operator's attention may be fully consumed with the mitigation of the cyber threat and the restoration of its services. However, operators are required to promptly notify the Authority of any cybersecurity incident that meaningfully threatened or compromised its networks, services or subscribers' information. Incidents may comprise unusual, non-routine attempts that were detected by their security detection and monitoring platforms and proactively extinguished before any network element or service was compromised, or constitute a full cyberattack, where services were either adversely affected or impaired; user or network elements were compromised by being infected with some form of malware; or inappropriate access was obtained.

Operators shall submit an incident report within five days of resolution where the incident is resolved within five days or, for an incident longer than five days, to notify the Authority, within seven days of the start of the incident, on the nature of the incident, the services impacted, the customers affected and how they were informed, the estimated timeframe for resolution of the incident, and any other matter the Authority may reasonably request or require, using the template in Appendix 1.

This threat information may be suitably anonymised and submitted to TT-CSIRT. This will allow TT-CSIRT to evaluate whether its threat assessment needs to be updated, and it will also enable other network operators to be notified, to ensure that their detection and protection mechanisms are in place.

Guidelines for Cybersecurity of Public Telecommunications Networks and Broadcasting Facilities (Required) – Reporting of Cyber Incidents

17. Operators of public telecommunications networks and broadcasting facilities shall promptly notify the Authority of any meaningful cybersecurity incident that occurs, whether the incident was unusual and addressed at the threat stage or involved the compromise or degradation of a network or user element and service, or user information.

18. Operators shall submit a full incident report to the Authority no later than five days of resolution where the incident is resolved within five days or, for incidents not resolved within five days, within seven days of the start of the incident, specifying the nature of the incident, the services affected, the scope of the impact of the incident, their customer notification plan, the timeframe for resolution of the incident, and any other matter the Authority may reasonably require.

All operators should have a set of common capabilities to support secure information sharing. Operators should be able to receive and act on threat information from other network operators and incident response organisations such as TT-CSIRT. Operators shall provide a point of contact for the exchange of cyber threat intelligence for the sharing of anonymised information on platforms that may be already established by TT-CSIRT. Mechanisms such as encryption should be used to secure the data being exchanged, as well as to provide for authentication of the sender to the recipient, to avoid phishing or other impersonation attacks.

Operators should establish internal policies on the classification, privacy and distribution of information, which should include requirements for the collection, use, retention and disposal of information, to ensure that the information exchanged is treated sensitively and appropriately. Operators should further limit the information shared to personnel and systems that are required to use that information to prepare for or resolve issues, and avoid the sharing of identifying information, either in terms of the operator reporting the incident or the personal information of the customers impacted (CSTAC 2013).

Guidelines for Cybersecurity of Public Telecommunications Networks and Broadcasting Facilities (Recommended) – Reporting of Cyber Incidents

19. Operators should share information among operators and incident response organisations, by securing the data exchanged and validating the source of the information.

20. Operators should ensure that the information received is appropriately handled, by establishing suitable internal policies on the treatment of such information.

4.8 Supply Chain and Vendor Management

Public telecommunications network operators generally deal with supply chain risks by extending their security controls and policies to the third parties they work with, particularly those from whom they source equipment and services. Many of these arrangements may present security risks that need additional mitigations, such as the outsourcing of network design, and the building and operation of telecommunications networks (Ofcom 2017).

Operators should ensure they undertake appropriate security risk assessments for any significant vendor arrangements. Suitable processes should be implemented for the ongoing management of identified risks. Operators should also make reasonable efforts to ensure that network equipment procured and installed within their networks is secure.

Consequently, operators should:

1. define security standards for the procurement of systems, services, devices and software that comply with such standards that may be established by the Authority.

2. ensure that relevant security standards are included in purchase agreements and requests for proposals.

3. require third parties to test and verify that all equipment, software and systems are in accordance with established security best practices.

4. establish procedures to ensure that vendors follow standards defined by network operators.

5. support a verification programme to ensure that vendors, particularly of critical infrastructure, follow the standards defined by the network operators.

6. limit vendor access to only those systems for which vendors provide support.

7. ensure the integrity and security of their networks, by monitoring and logging vendor activity.

8. ensure that security hardening requirements are included in service level agreements with third party vendors.

9. ensure that mechanisms of support during cybersecurity incidents are included in service level agreements.

Guideline for Cybersecurity of Public Telecommunications Networks and Broadcasting Facilities (Recommended) – Supply Chain and Vendor Management

21. Operators of public telecommunications networks and broadcasting facilities should establish and implement appropriate mechanisms to ensure their significant vendors, and the equipment, software and systems supplied, are secure and are monitored to ensure continued security, in accordance with standards that may be established by the Authority.

4.9 Subscriber Privacy and Data Protection

The privacy rights of subscribers are enshrined under section 4(c) of the Constitution of Trinidad and Tobago and are intended to be further defined under the Data Protection Act. Those legal requirements take full precedence over these guidelines. Public telecommunications network operators are also expected to maintain the same level of commitment to their customers with respect to privacy.

Specifically, the sharing of personal information is rarely needed for abuse or trouble resolution. The network operator serving a customer must be able to identify the user who is infected or perpetrating abuse activities, but this information should not be shared with other entities unless the disclosure is done in accordance with the requirements of the provider's privacy policies and the terms and conditions of service, or as otherwise stated in written law.

While the relevant legislation outlines the privacy rights of citizens, along with the responsibilities that network operators have in protecting those rights, network operators should ensure that the services, systems and processes they provide adhere to all applicable privacy legislation. They should deal with privacy concerns promptly and transparently and evaluate any actions to secure their network to protect the privacy rights of their subscribers.

Guideline for Cybersecurity of Public Telecommunications Networks and Broadcasting Facilities (Required) – Subscriber Privacy and Data Protection

22. Operators of public telecommunications networks and broadcasting facilities shall ensure the privacy rights of their subscribers are protected, in accordance with all applicable legislation in effect, and address privacy concerns promptly and transparently.

4.10 Cybersecurity Awareness, Education and Training

Public telecommunications operators are expected to provide cybersecurity awareness training to their personnel. All relevant employees should possess the appropriate awareness, knowledge and skills necessary to perform their tasks with cybersecurity risks in mind (NIST 2024). Staff should be able to positively contribute to the cybersecurity of essential functions. Cyberattacks may appear on customers' devices as attractive incentives that require personal or financial information to be submitted. Through awareness campaigns highlighting the dangers of cyberattacks, consumers should be made aware of what they should and should not do in relation to submitting personal information or financial data online.

The *Cyber Assessment Framework* of the National Cyber Security Centre (NCSC) outlines desirable outcomes relating to a cybersecurity culture and training. These are summarised as follows (NCSC 2022):

1. Executive management should be able to communicate cybersecurity priorities unambiguously to all members of staff, who should display positive attitudes, behaviours and expectations with respect to cybersecurity.

2. Staff members who raise potential cybersecurity risks should be treated positively. Staff should routinely report any concerns related to cybersecurity and should be recognised for their contribution. Management should be actively involved in upkeeping and improving cybersecurity.

3. There should be open communication about cybersecurity among staff, with any concerns being taken seriously. People across the organisation should be involved in cybersecurity activities to build joint ownership and contribute from the perspective of their area of expertise.

4. Staff should follow appropriate cybersecurity training paths. Staff cybersecurity training should be tracked and refreshed at intervals. Cybersecurity training and awareness activities should be evaluated routinely to ensure effectiveness and wide reach.

5. Information and guidelines on cybersecurity and good practices should be easily accessible, widely available and knowingly referenced, and followed throughout the organisation.

6. Operators should make available to their customers information advising on how to safely use their services, and how to protect themselves from cyber threats and attacks.

Guidelines for Cybersecurity of Public Telecommunications Networks and Broadcasting Facilities (Recommended) – Cybersecurity Awareness, Education and Training

23. Operators of public telecommunications networks and broadcasting facilities should ensure that all members of staff undergo appropriate cybersecurity training relevant to their field of work. Cybersecurity training programmes should be routinely evaluated to ensure they are kept up to date and effective.

24. Members of staff should receive updates on cybersecurity priorities, incidents or any other relevant information, through any appropriate means, including briefings.

25. Staff should be provided with all the tools necessary to fulfil their responsibilities while applying the company's cybersecurity protocols.

26. Operators of public telecommunications networks and broadcasting facilities should inform their customers on how to securely use their services.

4.11 Monitoring and Conformance

In accordance with the relevant section A28 (TATT 2007) of the concessions granted, operators should prepare a report, for review annually by the Authority and in the format defined by the Authority, that indicates their level of conformance with these cybersecurity guidelines. A sample format is included in Appendix II. Operators should also indicate in their submission the timeframe to comply with a required guideline, or conform with a recommended guideline, to which they currently do not adhere.

This annual report should state, for each guideline, whether the operator is fully conformant, partially conformant, or non-conformant, or if the guideline is not applicable to their operations. The Authority does not consider a summary of the status of conformance with the guidelines as confidential information but, rather, as information that should be available to consumers and may be published by the Authority. Section A25 of the concession (TATT 2007) states:

> In the event of a material breach of the Act, regulations, instruments or directions made under the Act, or any condition of this Concession, the Authority or the Minister, whichever is appropriate in accordance with the relevant provisions of the Act, may:
>
> a. suspend or terminate this Concession or the concessionaire's right to operate any network or provide any service under this Concession; or,
>
> b. take such other action as it deems appropriate;
>
> in accordance with the relevant provisions of the Act and any regulations.

Failure to submit the conformance report, or failure to comply with a required guideline, which is a guideline that an operator shall perform or is required to satisfy, may be deemed a breach of concession and the Authority shall act as prescribed under the concession or the Act.

While full conformance with all new cybersecurity standards is encouraged, the Authority recognises that the cost of upgrading certain legacy networks may be prohibitive. Operators of legacy networks, however, are expected to implement the Authority's guidelines that are applicable, while demonstrating that key vulnerabilities to cyberattacks in their networks are being addressed to acceptable levels, using appropriate measures, as part of their conformance report submission.

Guideline for Cybersecurity of Public Telecommunications Networks and Broadcasting Facilities (Required) – Monitoring and Conformance

27. *Operators of public telecommunications networks and broadcasting facilities shall submit an annual conformance report stating whether they are fully conformant, partially conformant or non-conformant with each cybersecurity guideline, or if the guideline is not applicable to their operations. Failure to submit the annual conformance report or comply with a required guideline may be deemed as a breach of concession and the Authority shall act as prescribed under the concession or the Act.*

References

CBTT. 2023. *Cybersecurity Best Practices Guideline.* Policy guideline, Port of Spain. https://www.central-bank.org.tt/sites/default/files/page-file-uploads/cybersecurity-best-practices-guideline-09132023.pdf: Central Bank of Trinidad and Tobago.

CSTAC. 2013. *Security Best Practices for Canadian Telecommunications Service Providers (TSPs).* Canada: Canadian Security Telecommunications Advisory Committee.

EBU. 2024. *R 143 v2.4 - Cybersecurity Recommendation for Media Vendors' Systems, Software & Services.* European Broadcasting Union.

ENISA. 2021. *Guidelines on Security Measures under the EECC.* Technical Guidance, Europe: ENISA.

GoRTT. 2012. *National Cyber Security Strategy.* Port of Spain. https://ttcsirt.gov.tt/wp-content/uploads/2022/04/National_Cyber_Security_Stategy_2012.pdf: Government of the Republic of Trinidad and Tobago.

GSMA. 2024. *GSMA Baseline Security Controls Version 3.0.* GSM Association.

ISO/IEC. 2022. *ISO/IEC 27001 - Information Security, Cybersecurity and privacy protection Requirements.* Standard, Geneva, Switzerland: ISO/IEC.

ITU. 2009. *Cybersecurity: The Role and Responsibilities of an Effective Regulator.* Switzerland: International Telecommunication Union.

ITU. 2023. *ITU-T Recommendation X.1051 - Information Security, cybersecurity and privacy protection – Information security controls based on ISO/IEC 27002 for telecommunications organisations.* Recommendation, Geneva: International Telecommunication Union.

ITU. 2015. *Security in Telecommunications and Information Technology.* Report, Switzerland: International Telecommunication Union.

MAGLA. 2011. *Data Protection Act.* Legislation, Port of Spain: Ministry of Attorney General and Legal Affairs, Government of Republic of Trinidad and Tobago.

NAB. 2016. *The Essential Guide to Broadcasting Cyber Security.* Washington D.C.: National Association of Broadcasters.

NCSC. 2022. *Cyber Assessment Framework V3.1.* London: National Cyber Security Centre.

NESAS. 2023. *Network Equipment Security Assessment Scheme - Overview.* Technical Document, GSM Association.

NIST. 2024. *The NIST Cybersecurity Framework (CSF) 2.0.* Gaithersburg: National Institute of Standards and Technology.

Ofcom. 2017. *Ofcom guidance on security requirements in sections 105A to D of the Communications Act 2003.* United Kingdom: Ofcom.

TATT. 2007. *Concession for the Operation of a Public Telecommunications Network and/or Provision of Public Telecommunications and/or Broadcasting Services.* Barataria: Telecommunications Authority of Trinidad and Tobago.

TATT. 2021. *Procedures for Consultation in the Telecommunications and Broadcasting Sectors of Trinidad and Tobago.* Procedure, Barataria: Telecommunications Authority of Trinidad and Tobago.

TATT. 2004. *Telecommunications Act 2001 Chap 47:31.* Barataria: Telecommunications Authority of Trinidad and Tobago.

Appendix 1. Template for Reporting of Cybersecurity Incidents

Description	Value	Comments (if needed)
Operator name		
Operator incident reference number		
Date of occurrence		
Time of occurrence		
Resolution status		
Date of resolution		
Time of resolution		
Location of incident		
Brief description of incident		
Services impacted		
Number of customers affected		
Networks and assets affected		
Summary of incident cause		
Actions taken to date		
Name and contact details for updates		
Remaining known actions to be taken		
Indicators of compromised observed		
Tactics, techniques, and procedures (TTPs) observed		

Appendix ll: Template for the Reporting of Conformance with Cybersecurity Guidelines

Guideline No.	Conformance Notation	Guideline	Applicable (Yes or No)	Level of Conformance with Guideline if Applicable Indicate Using (✓)		
				Fully Conformant	Partially Conformant	Non-conformant
Critical Network Infrastructure						
1	Recommended	Operators of public telecommunications networks and broadcasting facilities are urged to adopt the ISO 27001 standard on information security management system requirements under the controls specified in ITU-T Recommendation X.1051, to protect their critical network infrastructure.				
2	Recommended	Operators of public telecommunications networks and broadcasting facilities should possess the capability to: 1) restrict, monitor and log management access to approved hosts and services. 2) log and monitor critical events for network elements. 3) implement mechanisms to protect control channels and signalling traffic. 4) secure all critical core network elements. 5) ensure network elements are maintained at their most secure versions.				

3	Recommended	Operators of public telecommunications networks based on IP should deploy secure and resilient DNS infrastructure and services, according to industry-recognised standards, to protect their own domain and the domains for which they are responsible.				
Network Security Monitoring and Detection						
4	Recommended	Operators of public telecommunications networks and broadcasting facilities should monitor network traffic to detect malicious behaviour and activity, including through volumetric monitoring.				
5	Recommended	Operators should protect critical assets from internal and external threats.				
6	Recommended	Operators should maintain security information and event management systems that collect and correlate information from their various devices and platforms.				
7	Recommended	Operators should log, monitor and identify the source of malicious and abnormal traffic, through signature, heuristic, and volume characteristics.				
8	Recommended	Operators should monitor and log traffic flows and volumes from internal users and public customers to critical network infrastructure and its services.				
9	Recommended	Operators should monitor for, and log the misuse of, email service provision and high volumes of spam-related traffic, emanating from the hosted services provided to their customers.				
Responsible Use and Delivery of Messaging Services						

10	Recommended	Public telecommunications network operators should implement suitable mechanisms to mitigate the use of SMS for cyberattacks, including, but not limited to, the mitigation of SMS spamming.				
11	Recommended	Public telecommunications network operators should not use SMS for the transmission of sensitive, persistent user credentials and sensitive personal financial information, such as credit card numbers, to enable their customers to access their operator accounts.				
User and Network Interconnection						
12	Recommended	Operators of public telecommunications networks and broadcasting facilities should implement appropriate security measures for user connectivity and network interconnection, to protect end users, their networks and interconnected networks.				
Incident Response Capability and Preparation						
13	Required	Operators of public telecommunications networks and broadcasting facilities shall be able to respond to threats and attacks they detect through their monitoring programme. Their response shall be well defined and documented and include how the impact of the incident will be contained, how services will be restored, and how customers will be notified.				
Development and Maintenance of Cybersecurity Plans						
14	Required	Operators of public telecommunications networks and broadcasting facilities shall prepare and submit to the Authority their cybersecurity plan, or suitable independent certification of its existence, within one year of being directed to do so by the Authority.				

15	Required	Operators shall review this plan at least annually, or when a major threat is identified, to ensure it is relevant to the threat assessment of TT-CSIRT or other recognised cybersecurity authority.				
16	Recommended	Operators should conduct annual independent testing of their networks and related systems under the plan, which can include simulations, vulnerability assessments, security penetration testing, governance and access control reviews, and security monitoring and detection audits.				
Reporting of Cyber Incidents						
17	Required	Operators of public telecommunications networks and broadcasting facilities shall promptly notify the Authority of any meaningful cybersecurity incident that occurs, whether the incident was unusual and addressed at the threat stage or involved the compromise or degradation of a network or user element and service, or user information.				
18	Required	Operators shall submit a full incident report to the Authority no later than five days of resolution where the incident is resolved within five days or, for incidents not resolved within five days, within seven days of the start of the incident, specifying the nature of the incident, the services affected, the scope of the impact of the incident, their customer notification plan, the timeframe for resolution of the incident, and any other matter the Authority may reasonably require.				
19	Recommended	Operators should share information among operators and incident response organisations, by securing the data exchanged and validating the source of the information.				

20	Recommended	Operators should ensure that the information received is appropriately handled, by establishing suitable internal policies on the treatment of such information.				
Supply Chain and Vendor Management						
21	Recommended	Operators of public telecommunications networks and broadcasting facilities should establish and implement appropriate mechanisms to ensure their significant vendors, and the equipment, software and systems supplied, are secure and are monitored to ensure continued security, in accordance with standards that may be established by the Authority.				
Subscriber Privacy and Data Protection						
22	Required	Operators of public telecommunications networks and broadcasting facilities shall ensure the privacy rights of their subscribers are protected, in accordance with all applicable legislation in effect, and address privacy concerns promptly and transparently.				
Cybersecurity Awareness, Education and Training						
23	Recommended	Operators of public telecommunications network and broadcasting facilities should ensure that all members of staff undergo appropriate cybersecurity training relevant to their field of work. Cybersecurity training programmes should be routinely evaluated to ensure they are kept up to date and effective.				
24	Recommended	Members of staff should receive updates on cybersecurity priorities, incidents or any other relevant information, through any appropriate means, including briefings.				

25	Recommended	Staff should be provided with all the tools necessary to fulfil their responsibilities while applying the company's cybersecurity protocols.				
26	Recommended	Operators of public telecommunications networks and broadcasting facilities should inform their customers on how to securely use their services.				