Code of Practice for Information Security, Cybersecurity and Privacy Protection for ICT/Telecommunication Service Providers

འབྲུག་བང་དོན་བཙུད་འཕེལ་དང་བང་བཙུད་དབང་འཛིན།

Bhutan InfoComm and Media Authority
Royal Government of Bhutan

Contents

1. Legal Basis

This Code of Practice is issued as per section 58 of the Information, Communications and Media Act of Bhutan 2018 to by the Bhutan Information Communication and Media Authority to have a standard code of practice for the ICT service providers in the field of information security, cybersecurity and privacy protection.

2. Title and Commencement

This Code shall be called the Cybersecurity Code of Practice for ICT/Telecommunications Service Providers and shall come into force on the 10th day of October, 2024 corresponding to the 7th day of the eighth month of the Bhutanese Wood Male Dragon Year.

3. Scope of Application

This code shall apply to the Telecom Service Providers and other ICT Service providers having critical information infrastructure.

4. Amendments

This Code is subject to amendment and changes in accordance with the needs and changes in national priorities, Government policies and industrial and technological trends. Amendment of this Code by way of addition, variation or repeal may be affected by the Authority as and when required.

5. Definitions

Act means the Information, Communications and Media Act of Bhutan, 2018.

Authority means the Bhutan InfoComm and Media Authority established as per the provisions of the Information, Communications and Media Act of Bhutan 2018.

Business Continuity Plan (BCP) means documented procedures that guide organizations to respond, recover, resume and restore businesses to a predefined level of operation following disruption and cover the resources, services and activities required to ensure the continuity of essential services.

Code means this Cybersecurity Code of Practice for ICT/Telecommunications Service Providers.

Cybersecurity means the "collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment, organization and users' assets. Organization and users' assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment".

Cybersecurity event means an observable occurrence of an activity in or through a computer or computer system that may affect the cybersecurity of that or another computer or computer system and includes a cybersecurity incident.

Disaster Recovery Plan (DRP) means a documented procedure which guides organizations on the steps to recover IT and/or OT capability when a disruption occurs.

Information and Communication Technology (ICT): the definition of an ICT shall be as defined in the Act.

ICT Facility or Facilities: the definition of an ICT facility or facilities shall be as defined in the Act.

Information Technology (IT) means an arrangement of interconnected computers that is used in the storing, accessing, processing, analyzing and sending of information.

Interested party stakeholder person or organization that can affect, be affected by, or perceive itself to be affected by a decision or activity.

Licensee means the ICT/telecommunications service providers who have obtained a license from the Authority.

Malicious software/firmware means software or firmware intended to perform unauthorized processes that will have adverse impact on the confidentiality, integrity, or availability of a computer system, for example: virus, worm, Trojan horse, spyware, info stealers and some forms of adware or other code-based entity that infects a host.

Non- Disclosure of Communications means a requirement not to disclose the existence, the content, the source, the destination and the date and time of communicated information.

Patch means a set of changes to a software or firmware that addresses its cybersecurity vulnerabilities, or other updates to its functionality, usability or performance.

Patch management means the process involving one or more of the following actions of acquiring, testing and installing patches or updates on existing software or firmware, enabling systems to stay updated, addressing vulnerabilities and includes patching applications, anti-malware, and firmware.

Penetration testing means an authorized process of evaluating the security of a computer system, network or application by finding vulnerabilities attackers could exploit and includes the process of:(a) gathering information about the target;(b) identifying possible entry points; (c) attempting to break in (either virtually or for real); and (d) reporting the findings.

Personnel means a person doing work under the organization's direction.

Personally identifiable information means any information that can be used to establish a link between the information and the natural person to whom such information relates, or can be directly or indirectly linked to a natural person.

Privilege means the rights assigned to any account including any user, application, service or system account.

Privileged account means any account including any user, application, service or system account, that has administrative access privileges.

Relevant Authorities means the governing body, regulatory Authority and law enforcement bodies mandated by the Act with respect to cybersecurity.

Remote access means an access to an ICT/telecommunication infrastructure by a user, or a process acting on behalf of a user, communicating through an external network.

Remote Facilities means computer or computer system that has remote access capability.

Residual risk means the risk exposure after risk mitigating controls is considered or applied.

Scenario-based cybersecurity exercise means an activity to assess and validate an organization's plans and capabilities relating to the handling of simulated cybersecurity incidents (the 'scenario') affecting the organization. The exercise scenario should be based on relevant threats. Depending on the nature of the threats, licensees may include social engineering and cyber range components in these scenarios.

Sensitive data means sensitive data including production data and system configuration information.

Strong encryption means industry-accepted standard algorithms to scramble data and encrypts/decrypts with a key to achieve data confidentiality.

Threat means "potential cause of unwanted incident, which can result in harm to a system or organization".

Threat hunting means the proactive effort to search for signs of malicious activity that has evaded security defenses within the organization.

Test environment means a setup of computer or computer systems to support test use cases.

Vendors include both technology suppliers and service providers.

Vulnerability means weakness of asset or control that can be exploited by one or more threats.

Vulnerability assessment means the process of identifying, assessing and ranking security vulnerabilities in a computer system.

6. Abbreviations

For the purposes of this cybersecurity code of practice, following abbreviations apply:

CIA	Confidentiality, Integrity and Availability
CISA	Certified Information Systems Auditors
CISO	Chief Information Security Officer
CIRT	Cyber Security Incident Response Team
CRISC	Certified in Risk and Information Systems Control
DDoS	Distributed Denial of Service
DNS	Domain Name System
DNSSEC	Domain Name System Security Extensions
DoS	Denial of Service
HVAC	Heating, Ventilation, and Air Conditioning
ID	Identity Document
IP	Internet Protocol
ISMS	Information Security Management System
NIDS	Network Intrusion Detection System
NIPS	Network Intrusion Prevention System
NMS	Network Management System
PII	Personally Identifiable Information
RBAC	Role Based Access Control
SOC	Security Operation Center
URL	Uniform Resource Locator
WAF	Web Application Firewall

7. Introduction

Information is critical to every organization. ICT/Telecommunication providers provide facilities to various user types to process, transmit and store information. This information could be personally identifiable information, or confidential private and business data. In all cases, the licensee shall;

a) ensure that the information is handled with the correct level of care and attention; and

b) ensure appropriate levels of protection are provided to ensure confidentiality, integrity and availability (CIA), with privacy and sensitivity being paramount.

7.1 Understanding the Needs and Expectations of Interested Parties

The licensee shall determine;

a) interested parties that are relevant to the information security management systems;

b) the relevant requirements of these interested parties;

c) which of these requirements will be addressed through the information security management system.

7.2 Determining the Scope of the Information Security Management System

The licensee shall determine the boundaries and applicability of the information security management system to establish its scope. When determining this scope, the licensee shall consider interfaces and dependencies between activities performed by the licensee, and those that are performed by the other organizations.

7.3 Information Security Management System

The licensee shall establish, implement, maintain and continually improve an information security management system, including the processes needed and their interactions, in accordance with the requirements of this document.

8. Cybersecurity Governance

8.1 Leadership and Oversight

The licensee shall be cognizant of role of leadership and commitment in its information and network security management and shall take measures not limited to the following;

a) ensuring the information security management system (ISMS) policy and the objectives are established and are in line with its strategic direction;

b) ensuring the integration of the information and network security requirements;

c) ensuring that the resources needed for the ISMS are available;

d) communicating the importance of effective information and network security management and of confirming to the information and network security management requirements;

e) promoting continual improvement; and

f) supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibilities.

8.2 Policies, Standards, Guidelines and Procedures

a) The licensee shall have governing processes in the form of policies, standards and guidelines in place.

b) The licensee shall coordinate and review the implementation of security across the organization. This is followed by mandatory standards for compliance, as well as recommended guidelines for best practice.

c) The licensee shall ensure that each policy, standard, guidelines and procedure have an owner who has approved management responsibility for the development, review and evaluation of the policies.

d) The licensee shall establish and implement policies, standards, guidelines and procedures for managing cybersecurity risks and protecting ICT facilities against cybersecurity threats. The policies, standards, guidelines and procedures shall be:

i. aligned with this code, sector regulatory cybersecurity requirements, and applicable sectoral or national cybersecurity policies, standards, directions and procedures; and

ii. published and communicated to all personnel and external parties who act on or have access to infrastructure.

e) The licensee shall review the policies, standards, guidelines and procedures against the current organization's cyber operating environment and cybersecurity threat landscape published by the relevant authorities at least once every 12 months.

e) The policies, standards, guidelines and procedure with respect to information and network security shall be made available as documented information, communicated within all staff of the licensee and made available to relevant stakeholders and interested parties, as appropriate.

8.3 Roles and Responsibilities

The licensee shall ensure that the responsibilities and authorities for roles relevant to information security are assigned and communicated. The licensee shall assign the responsibilities and authority for:

a) ensuring that the information and network security management system conforms to the policy, standards, guideline etc.;

b) reporting on the performance of the information and network security management system to top management.

c) reporting the performance of the information and network security management system within the organization and the following functions should be assigned in the applicable organization:

i. regulatory/authority contact;

ii. information and network security responsibility such as chief information security officer (CISO); and

iii. risk management.

8.4 Documented Operating Procedures

a) The licensee shall develop and implement documented operating procedures for information processing facilities and made available to personnel who need them.

b) The operating procedures shall specify;

   i. the responsible individuals;

   ii. the secure installation and configuration of systems including secure authentication setup as per the current international standards;

   iii. processing and handling of information, both automated and manual;

   iv. backup and resilience;

   v. instructions for handling errors or other exceptional conditions, which can arise during job execution;

   vi. support and escalation contacts including external support contacts in the event of unexpected operational or technical difficulties;

   vii. storage media handling instructions;

   viii. system restart and recovery procedures for use in the event of system failure;

   ix. the management of the audit trail and system log information and video monitoring systems;

   x. monitoring procedures such as capacity, performance and security;

   xi. maintenance instruction.

c) The documented operating procedures shall be reviewed and updated when needed. Any changes to documented operating procedures should be authorized. Where technically feasible, information systems should be managed consistently, using the same procedures and utilities.

d) The licensee shall also develop and implement the documented operating procedures on vulnerabilities and incident reporting mechanism from the reliable and reputed external sources including its customers.

8.5 Compliance of Information Security Management System

The licensee shall be bound by the laws of the land, which require compliance by identifying and understanding the regulatory, statutory and contractual obligations pertaining to information and network security, given below:

a) identify, document and keep up to date applicable legal, statutory and contractual obligations.

b) protect records/information, personal and sensitive data in accordance with legal, regulatory, contractual and business requirements.

c) procedures should be established in relation to management of intellectual property rights and use of proprietary software products.

d) records should be protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with legislative, regulatory, contractual and business requirements.

e) privacy and personally identifiable information should be ensured as required in relevant legislation and regulation, where applicable.

f) the licensee’s approach to managing information and network security and its implementation should be reviewed independently at planned intervals or when significant changes occur.

g) the licensee shall regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security requirements.

h) information systems should be regularly reviewed for compliance with the organization's information and network security policies and standards.

8.6 Privacy and Protection of PII (Personally Identifiable Information)

a) The licensee shall establish and communicate a topic-specific policy on privacy and protection of PII to all relevant interested parties.

b) The licensee shall develop and implement procedures for the preservation of privacy and protection of PII. These procedures shall be communicated to all relevant parties involved in the processing of personally identifiable information.

c) The licensee shall ensure:

   i. compliance with these procedures and all relevant legislation and regulations concerning the preservation of privacy and protection of PII requires appropriate roles, responsibilities and controls.

   ii. responsibility for handling PII to be dealt with taking into consideration relevant legislation and regulations.

   iii. appropriate technical and organizational measures to protect PII are implemented.

8.7 Non-disclosure of Communications

The licensee shall take account of following guidelines:

a) maintaining ICT facilities properly to ensure non- disclosure of communications;

b) prohibiting the unauthorized or unlawful utilization of staff of the organizations of any information related to customer communications;

c) setting the appropriate retention period of data, which is within the time period required for carrying out the purposes for retaining data, and delete them at the end of retention period or at the attainment of the purposes without any delay;

d) prohibiting the provision of PII in communications to third parties, without legal enforcement or consent of ICT services users themselves;

e) When ICT service providers are requested to submit information related to ICT service users including non-disclosure of communications, the licensee shall need to confirm that request from law-enforcement agencies or other investigative bodies has gone through a legitimate procedure in accordance with the applicable laws and regulations.

8.8 Outsourcing and Vendor Management

a) The licensee shall be responsible and accountable for the cybersecurity of its network and ICT facilities even if the licensee outsources any functions, activities or operations to the external party or vendors.

b) The licensee shall establish processes and mechanisms to minimize cybersecurity risk arising from such outsourcing.

c) The licensee shall enter agreement(s) with the external party while outsourcing to external vendors and terms and conditions of the agreement shall ensure the cybersecurity of the infrastructure and it also include provisions to;

   i. reduce or mitigate the impact of any cybersecurity risks associated with the outsourcing; and

   ii. reduce risks associated with the external party's access to the infrastructure.

d) The licensee shall be able to incorporate changes in terms of its agreement(s) with external parties in the event of new legal or regulatory requirements.

9. Operational Planning and Control

9.1 Asset Management

a) The licensee shall establish mechanisms and processes to identify all critical assets and maintain an inventory of the assets. The inventory shall include the following:

   i. owner and/or operator of each asset;

   ii. name and description of each asset;

   iii. description of critical functions of each asset;

   iv. the dependencies of each asset and the connections between each asset and any systems or networks;

   v. physical location of each asset;

   vi. outsourced service providers used to support each asset;

   vii. cloud services used to support each asset.

   viii. information on the distributed denial-of-service (DDoS) attack mitigation measures in place for these internet links; and

   ix. network topology diagram, including the network perimeter, and all external computers and computer systems that the interfaces with.

b) The licensee shall update the inventory whenever there is any change to any asset of the licensee or to the information to be recorded in the inventory.

9.2 Risk Management

a) The licensee shall have the following plan:

   i. promotion of a "risk culture" that enables its personnel to have open communications about risk, make informed decisions about addressing risks based on learning from past experience, and carry out risk management efforts;

   ii. the roles and responsibilities of various persons responsible for managing cybersecurity risks to the ICT facilities and their governance structure, including their reporting lines and accountabilities;

   iii. cybersecurity risk assessment methodology;

   iv. processes for the monitoring, communication and reporting of cybersecurity risks in a timely manner to the management of the organization so that it can ensure that the necessary cybersecurity measures to address the risks are implemented;

   v. its cybersecurity risk criteria and thresholds or limits for residual risk.

b) The licensee shall include the following steps in the cybersecurity risk assessment methodology;

   i. risk identification – identification of critical assets and cybersecurity threats, including threats identified from threat modeling, threat hunting, post-incident reviews of cybersecurity incidents, and the construction of risk scenarios;

   ii. risk analysis – analysis of each risk scenario to determine the likelihood of occurrence and potential impact;

   iii. risk evaluation – determining, documenting and prioritizing risks; and

   iv. risk response – treatment and monitoring of each risk to keep the risk level within the licensee's risk tolerance level.

c) The licensee shall maintain and keep updated a risk register for each infrastructure. The risk register shall include the following:

   i. risk scenarios;

   ii. dates when the risk scenarios are identified;

   iii. existing measures in place to address the risk scenario;

   iv. risk treatment plan;

v. progress status of the treatment plan;

vi. residual risk ratings; and

vii. risk owner.

e) The licensee shall ensure that the person tasked with conducting the risk assessment for the ICT facilities is supervised or guided by an individual possessing industry-recognized certification, focused fully or in big scope on Information Risk Management, such as Certified in Risk and Information Systems Control (CRISC) or similar certification.

9.3 Business Continuity Plan

a) The licensee shall establish an effective Business Continuity Plan ("BCP") or Disaster Recovery Plan("DRP") to ensure availability and continuity operations in emergency situations like in the event of disruption due to a cybersecurity incident & etc.

b) The licensee shall review, verify and evaluate BCP or DRP and other related plans at regular intervals (at least once every 12 months) to ensure their effectiveness and validity.

c) The licensee shall ensure that the information processing facilities are implemented with redundancy sufficient to meet availability requirements.

9.4 Backup and Restoration Plan

a) The licensee shall establish a backup and restoration plan to ensure that its critical assets can be recovered in the event of system disruption or data corruption.

b) The licensee shall perform periodic backups at a frequency that is commensurate with the organization's operational requirements and ensure that the backups are completed successfully.

c) The licensee shall ensure that as far as feasible the backups that are stored on devices are not connected to any computer or the internet and are separated from the critical assets. If the backups that are stored on devices need to be connected to computers or the internet, the licensee shall ensure that backups stored on devices are protected from unauthorized access, modification and deletion.

d) The licensee shall test the restoration of the backups periodically to ensure that they can be restored when required.

e) The licensee shall review the backup and restoration plan at least once every 12 months to ensure that the plan remains relevant.

9.5 Access Control

a) The licensee shall implement RBAC (role- based access controls) by ensuring the access to ICT facilities and between parts of the infrastructure is restricted to authorized personnel, activities, processes and devices, with a limited number of profiles and controlled sets of user access permissions as applicable.

b) The licensee shall ensure that all vendors' access to its ICT facilities are:

    (i) documented and pre-approved;

    (ii) supervised by the organization;

    (iii) performed on-site.

c) The licensee shall implement mechanisms for timely tracking of access control by the vendors for the necessary amendments and timely removal of the access whenever and wherever necessary.

9.6 User Access Management

a) The licensee shall implement a process for user registration and deregistration to enable assignment of accounts and access rights.

b) The licensee shall implement a process for user access provisioning to assign or revoke access rights for all types of users, systems and services.

c) With respect to privileged accounts, the licensee shall:

    i. ensure that privileged access (i.e., administrative access) is granted only to selected accounts authorized to have such access;

    ii. maintain an updated inventory of privileged accounts including details of the permissions and privileges assigned to each account; and

    iii. implement multi-factor authentication where privileged accounts are used to access the infrastructure, and set up a mechanism like the user needs to seek and obtain additional permissions on a system or network after an initial log-in.

d) The licensee shall ensure that privileged access is initiated from a secure cyber environment and transfer of data takes place over authorized connections.

e) The licensee shall also ensure:

i. the allocation of secret authentication information is controlled through a formal management process;

ii. users are be required to adhere to an organization's practices in the use and management of secret authentication information;

iii. asset owners to formally review user's access rights at regular intervals; and

iv. a formal process to remove access rights of all employees and external party users to information, systems, infrastructure and services upon termination of their employment, contract or agreement, or adjust upon change is implemented and managed.

9.7 Domain Name System Security Extension (DNSSEC)

a) The licensee shall enable DNSSEC validation for its DNS resolvers, or implement any equivalent or better methods of validating the integrity of DNS records, to prevent DNS attacks such as DNS cache poisoning and DNS spoofing.

b) The licensee shall ensure that all domain names under its control and used in connection with the ICT facilities, including in the operation of the ICT facilities and in the delivery of services, are DNSSEC- signed on the corresponding DNS Authoritative Server for each domain name.

Note: DNSSEC is a security feature of DNS which validates DNS information (e.g. IP address) for a given domain name by adding cryptographic signatures to existing DNS records. This allows for the validation of the authenticity and message content integrity of DNS records.

9.8 Network Security

a) The licensee shall establish and implement network access control policy for the ICT facilities and perform periodic reviews to ensure they remain appropriate and up-to-date.

b) The licensee shall ensure the interconnection of its ICT facilities to any outside network is restricted and controlled except where necessary for operation of the ICT facilities and services. Where such interconnections are necessary, the licensee shall:

   i. implement network security mechanisms between the ICT facilities and the network to detect and block malicious network traffic and to secure network communications; and

   ii. restrict the direction of data flow to only one-way if only one-way data flow is required for the operations.

c) The licensee shall ensure that connection of the ICT facilities to the internet is restricted and controlled except where necessary for operating the infrastructure. Where connection to the internet is necessary, the licensee shall implement appropriate measures to mitigate and reduce cybersecurity risks arising from any such connection.

9.9 Segregation of Networks

a) The licensee shall segregate its network architecture into different network segments based on their different security and risk levels. The segregation can be done using either physically different networks or by using different logical networks.

b) The licensee shall limit any communications between the different network segments of ICT facilities to only the minimum necessary for operating the ICT facilities.

c) The licensee shall:

   i. implement network security mechanisms between the different network segments of the ICT facilities to detect and block malicious network traffic and to secure network communications; and

   ii. establish mechanisms and processes to isolate affected network segments of the ICT facilities in the event of a cybersecurity incident.

   iii. review and carry out auditing of deployed and expected segregation rules in the system configuration at least once every 12 months to ensure that the system is well managed.

9.10 System and Application Security

a) The licensee shall ensure;

   i. access to systems and applications shall be restricted in accordance with the access control policy of the organization.

   ii. access to systems and applications shall be controlled by a secure log-on procedure where required by the access control policy.

b) The licensee shall review the list of approved applications at least once every 12 months.

c) The licensee shall implement multi-tier architecture that separates the application and database tiers and implement security controls at each tier.

d) The licensee shall implement a Web Application Firewall (WAF) to monitor for detect and block web application threats to its system.

9.11 Secure Coding

a) The licensee shall ensure secure coding standards while planning and before coding.

b) The licensee shall prohibit the use of insecure design techniques (e.g. use of hard-coded passwords, unapproved code samples and unauthenticated web services).

c) The licensee shall conduct an analysis of the most common programming errors and document that these have been mitigated.

d) The licensee shall also ensure that updates are securely packaged and deployed, source code are protected against unauthorized access and tampering (e.g. by using configuration management tools, which typically provide features such as access control and version control).

e) The licensee, while using the external tools and libraries, shall ensure the software is maintainable, traceable and originates from proven, reputable sources.

9.12 Remote Access Management

a) The licensee shall put in place effective cybersecurity measures for all remote access to the ICT facilities to prevent and detect unauthorized access, and to validate that all such remote connections are authorized.

b) The licensee shall ensure that multi-factor authentication is required for establishing a remote access to the ICT facilities and remote connections to the ICT facilities have strong encryption and are made only through secured intermediary mechanisms.

c) The licensee shall put in place that measures to ensure transmission security and message integrity over the remote connection and data flows over remote connections to the ICT facilities are limited to only the minimum necessary for performing the function required of the connection.

d) The licensee shall ensure files to be uploaded to the ICT facilities are scanned for malware before being uploaded.

9.13 Patch Management

a) The licensee shall establish and implement a security patch management process including the monitoring the release of security patches for licensee's assets, verifying the integrity of the security patches, testing security patches to ensure that the patches do not negatively affect the operations and cybersecurity of the licensee.

b) The licensee shall prioritize the application of security patches based on the level of risk posed to the operations of the ICT facilities and apply security patches in a timely manner to reduce cybersecurity vulnerabilities.

c) The licensee shall also monitor and track the progress of patching and apply compensating controls to mitigate and reduce cybersecurity risks in cases where a security patch cannot be applied.

d) The licensee shall ensure that there is management oversight over the effectiveness of the security patch management processes.

9.14 Malicious Software/Firmware Protection

a) The licensee shall implement the rules and controls that prevent or detect the use of unauthorized software (e.g. application allowlisting i.e. using the list providing allowed applications).

b) The licensee shall implement controls that prevent or detect the use of known or suspicious malicious websites (e.g. blocklisting) on its DNS network.

c) The licensee shall install and regularly update malware detection and repair software to scan computers and electronic storage media.

d) The licensee shall determine the placement and configuration of malware detection and repair tools based on risk assessment outcomes.

e) The licensee shall prepare appropriate business continuity plans for recovering from malware attacks, including all necessary data and software back up (including both online and offline backup) and recovery measures.

f) The licensee shall isolate environments where catastrophic consequences can occur.

g) The licensee shall define procedures and responsibilities to deal with protection against malware on the system, including providing training and awareness to all users in their use, reporting and recovering malware attacks.

9.15 Response to DoS/DDoS attacks

a) The licensee shall stipulate the policies or procedures for responding to DoS/DDoS attacks and implement appropriate controls.

b) When a licensee recognizes the incidence of DoS/DDoS attacks e.g., detection of abnormal traffic patterns and unstable operation status of ICT facilities, the licensee shall take appropriate countermeasures in order to ensure the continuous and stable operations of ICT facilities.

c) Although specific measures required depend upon the type of DoS/DDoS attacks, the licensee shall take account of the following countermeasures:

   i. filtering of packets heading for the target set under attack;

   ii. restriction of communication port used for DoS/DDoS attacks;

   iii. reduction or suspension of operation of target ICT facilities.

9.16 Cryptographic Key Management

a) The licensee shall develop the policy on the cryptographic controls for the protection of information and it shall be based on the requirements from the relevant regulatory bodies and other industry requirements.

b) The licensee shall ensure that all cryptographic keys for the organization are protected against unauthorized access.

c) A cryptographic key management policy on the use, protection and lifetime shall be developed and implemented to manage its life cycle. The licensee shall review these mechanisms and processes at least once every 12 months to ensure their continued effectiveness.

10. Physical and Environmental Security

10.1 Physical Security Perimeter

The licensee shall consider and implement the following guidelines where appropriate for physical security perimeters:

a) ICT operation centers shall be equipped with adequate physical intruder detection systems;

b) Facilities for ICT services shall be physically separated and sited away from other facilities, e.g., customer facilities in managed data centers;

c) Physical barriers shall be effectively installed, with all local security policies rigorously enforced to ensure the protection of information and other associated assets at all times; if a physical barrier is malfunctioning or policy is not followed, it is imperative that the issue be resolved immediately by management with the appropriate level of responsibility.

10.2 Physical Entry

The licensee shall consider the following guidelines;

a) Appropriate physical security controls shall be applied to all ICT operations rooms and controls centers;

b) Upon entry, relevant visitor card data shall be recorded and adequately protected from unauthorized disclosure;

c) Visitor records shall be physically and electronically protected to preserve the CIA of the information they contain.

10.3 Securing Equipment Room

The licensee shall consider and implement following guidelines for securing the ICT equipment room:

a) the equipment room shall not be located where it is susceptible to external effects, such as natural disasters;

b) the equipment room shall be located where it is least susceptible to intrusion by unauthorized personnel- adequate measures shall be taken to prevent such intrusions;

c) the equipment room shall be located where it is least susceptible to damage from strong electromagnetic fields. If the room needs to be located where it is susceptible to strong electromagnetic fields, it should be protected by electromagnetic shields or some other measures;

d) important facilities shall be placed in an exclusive equipment room with appropriate physical protection;

e) materials used for floor, walls, ceiling etc. shall be non-combustible or fire-resistant;

f) the equipment room shall be air conditioned;

g) fire extinguishers, including the automatic fire alarm system shall be installed in the equipment room and the air-conditioning facility room;

h) HVAC controls shall be connected to an uninterruptible power supply to ensure loss of power does not impact the operating environment.

11. Performance Evaluation and Detection

11.1 Monitoring and Detection

a) The licensee shall establish and implement mechanisms and processes for the purposes of monitoring and detecting all cybersecurity events in respect of the organization.

b) The licensee shall collect and store records of all such cybersecurity events (including, where available, logs relating to the cybersecurity event) and implement the mechanism and processes for the purpose of triggering applicable incident reporting, response and recovery plans if there is or has been any cybersecurity incident.

c) The licensee shall establish and implement the mechanisms and processes for monitoring and detecting cybersecurity events and shall include following processes:

   i. recording of IP addresses, Uniform Resource Locator (URL), domains and hashes;

   ii. establishing the daily routine for monitoring of operational activities and network traffic in the ICT facilities, and

   iii. ensuring that alerts for further investigation are triggered for all deviations and anomalous activities that are detected.

d) The licensee shall review the mechanisms and processes established under clause 11.1(c) at least once every 12 months to ensure that the mechanisms and processes remain effective for their purposes.

11.2 Logging

a) The Licensee shall generate, collect and store logs to record system activities, exceptions, remote connections, network connections, faults and security events.

b) The Licensee shall also generate, collect and store the following categories of logs;

   i. network Firewall logs;

   ii. Domain Name System (DNS) logs;

   iii. web Proxy logs; and

   iv. Network Intrusion Detection/Prevention System (NIDS/NIPS) logs.

c) These logs under clause 11.2(b) shall contain information to provide visibility of network activities within the organization's infrastructure and between the organization's ICT facilities and networks outside of the organization.

d) The licensee shall ensure that the logs generated, collected, and stored under clause 11.2(b) use a consistent time source, are protected against unauthorized access, modification and deletion and logs are stored for the minimum period of 2 months after the date of event to which the log relates.

e) The licensee shall also ensure that the logs generated, collected and stored are governed by a log retention policy to facilitate investigations into cybersecurity incidents, the conduct of threat hunting, and any other purposes relating to the cybersecurity of the organization.

f) The licensee shall provide any such logs as may be required by the Authority for threat monitoring, threat analysis, threat alerts, and incident response.

11.3 Information and Network Audit

The licensee shall conduct internal audits at planned intervals to provide information on whether the information and network security management system:

a) conforms to:

   i. the licensee's own requirements for its information and network security management system (recommendation standard for auditing is attached in annexure 1); and

   ii. the requirements of this document including standards, guidelines, directives on requirement and etc. set by the Authority related to information and network auditing;

b) is effectively implemented and maintained.

The licensee shall:

a) plan, establish, implement and maintain an audit program(s), including the frequency, method, responsibilities, planning requirements and reporting. The audit program(s) should take into consideration the importance of the processes concerned and the result of the previous audit;

b) define the audit criteria and scope of each audit;

c) select auditors and conduct audits that ensure objectivity and the impartiality of the audit process;

d) ensure that any person or group of persons tasked with conducting the cybersecurity for an ICT facility is supervised or guided by an individual possessing industry-recognized certification, such as Certified Information Systems Auditor (CISA) or similar certification.

e) ensure that the results of the audits are reported to the relevant management; and

f) retain documented review information as evidence of the audit program(s) and the audit results.

11.4 Remediation of Audit Findings

a) Where any audit identifies any non-compliance by a licensee with the requirements specified in the Act or any codes of practice or standards of performance issued under the Act, the licensee shall, unless the Authority indicates otherwise in writing, submit an audit finding remediation plan to the Authority within 30 working days from the date that the licensee receives the audit report.

b) The audit finding remediation plan shall:

   i. have detail remediation actions which the licensee will take to address each area of non-compliance; and

   ii. set out the timeline(s) for implementing the actions stated in sub-clause (a).

c) The licensee shall implement the audit finding remediation plan and complete all remediation actions within the timeframe(s) specified in the said plan, to the Authority's satisfaction, and at the licensee's own cost. The licensee then shall update the Authority when each remediation action is completed.

11.5 Vulnerability Assessment

a) The licensee shall establish a mechanism to identify and track cybersecurity vulnerabilities of the organization's ICT facilities.

b) The licensee shall institute measures to remediate all cybersecurity vulnerabilities in a timely manner, with priority given to vulnerabilities that pose a greater risk to the security or operations of the ICT facilities.

c) The licensee shall conduct a vulnerability assessment at least once every 12 months.

d) The licensee shall also conduct a vulnerability assessment for relevant organization's assets after implementing any major system changes like commissioning new systems to be connected to the ICT facilities, implementing new application modules, system upgrades and technology refresh.

11.6 Penetration Testing

a) The licensee shall conduct a penetration test on its ICT facilities at least once every 12 months.

b) The licensee shall also conduct a penetration test for relevant organization's assets after implementing any major system changes like commissioning new systems to be connected to the infrastructure, implementing new application modules, system upgrades and technology refresh.

c) The licensee shall ensure that third-party penetration testing service providers and their penetration testers who are performing penetration tests possess industry-recognized accreditations and certifications respectively.

d) The licensee shall also ensure;

   (i) penetration testers performing the penetration tests must have industry- recognized penetration testing certification to demonstrate assurance of their knowledge and practical skills.

   (ii) service providers must have industry-recognized accreditation to demonstrate assurance of their policies and procedures in penetration testing service, reporting and data handling, and due diligence in hiring of ethical penetration testers.

e) The licensee shall ensure that all penetration tests by third-party service providers are conducted under supervision of the licensee to ensure that activities carried out by the

service providers are within the intended scope of the penetration test and do not disrupt operations of the ICT facilities and services.

11.7 Cybersecurity Information Exchange

a) The licensee shall establish and implement mechanisms and processes to obtain threat intelligence, and to process and analyze the threat intelligence for relevance and potential impact to the ICT facilities. Threat intelligence includes information on the current cybersecurity threat landscape; activities of threat actors; tactics, techniques and procedures of threat actors; and cybersecurity vulnerabilities.

b) The licensee shall establish and implement mechanisms and processes to share information on cybersecurity threats and vulnerabilities, and on measures that can be taken in response to such threats and vulnerabilities, with the relevant Authorities for threat monitoring and analysis.

c) The licensee shall put in place controls to mitigate cybersecurity threats and address vulnerabilities identified from threat intelligence.

12. Incident Response and Recovery

12.1 Incident Management and Security Operation Center (SOC)

a) The Licensee shall establish a Cybersecurity Incident Response Plan that sets out how a licensee should respond to a cybersecurity incident.

b) The licensee shall establish an organizational incident response team or Computer Incident Response Team ("CIRT") or Security Operation Center (SOC) to continuously monitor and mitigate security risk, threats and vulnerabilities.

c) The licensee shall ensure that the cybersecurity Incident Response Plan includes;

(i) an Incident Reporting structure which can guide the licensee on the compliance with respect to its reporting obligations under the Act and any other laws and regulations.

(ii) communication and coordination mechanism and procedures to ensure timely and effective cybersecurity incident management by the CIRT/SOC and the Management of the organization.

(iii) thresholds and procedures to activate the incident response and CIRT/SOC.

(iv) having post-incident review procedures by incorporating the lessons learnt including the holding a post- incident meeting with affected stakeholders, collecting data, such as total hours on involvement and costs, and use it for improvement of the incident management scheme.

d) The licensee shall ensure that the CIRT/SOC is trained and equipped with the necessary resources to respond to cybersecurity incidents.

e) The licensee shall establish and implement processes to identify, investigate and address the root causes that contributed to each cybersecurity incident, including any structural, behavioral, managerial, technical or systemic factors, so as to prevent recurrence of similar incidents.

f) The licensee shall review the Cybersecurity Incident Response Plan to ensure that it remains updated and relevant at least once every 12 months.

12.2 Cybersecurity Exercise

a) The Licensee shall conduct the scenario-based cybersecurity exercises at least once every 12 months.

b) The licensee shall include following elements while designing the incident response scenarios for the cybersecurity exercises;

   i. responses to identified threats and vulnerabilities;

   ii. coordination plans with relevant stakeholders (including the customers and vendors).

   iii. monitoring for further cybersecurity threats and incidents even during incident response.

c) The licensee shall ensure that the following stakeholders participate in the cybersecurity exercises:

   i. senior management;

   ii. incident management team;

   iii. CIRT/SOC;

   iv. business operation and communication staff of the organizations; and

   v. service providers.

13. Cybersecurity Training and Awareness

13.1 Cybersecurity Awareness Program

a) The licensee shall conduct a cybersecurity awareness program to its employees and relevant stakeholders (including external vendors).

b) The cybersecurity awareness program shall include;

   i. awareness of relevant laws, regulations, codes of practice, policies, standards, guidelines and procedures;

   ii. general cybersecurity awareness messages and prevailing cybersecurity threats, impacts and mitigations; and

   iii. awareness to promote cyber hygiene within the organization and with the relevant stakeholders.

c) The licensee shall review the cybersecurity awareness program at least once every 12 months to ensure that the program remains current and relevant.

13.2 Cybersecurity Capacity Building

a) The licensee shall design and execute a capacity building program related to cybersecurity to enhance employee's security skills.

b) The licensee shall ensure the employees conducting a cybersecurity risk assessment and internal cybersecurity audit for the organization are supervised and guided by a person with Certified in Risk and Information System control (CRISC) or equivalent and Certified Information Systems Auditor (CISA) or similar certification respectively.

Annexure 1: Guiding Documents for Information and Network Auditing for ICT/Telecommunications Service Providers.

It is recommended to use following standard documents as the guideline for the information and network auditing of licensee's ICT facilities or infrastructure:

1. ISO/IEC 27001:2022, Information security, cybersecurity and privacy protection- Information security Management systems- Requirements.

2. ISO/IEC 27002:2022, Information security, cybersecurity and privacy protection- Information security controls.

3. ISO/IEC 27005:2022, Information security, cybersecurity and privacy protection- Guidance on managing information security risks.

4. ITU-T Recommendation X.1051(2023): Information security, cybersecurity and privacy protection- Information security controls based on ISO/IEC 27002 for telecommunications organizations. https://www.itu.int/rec/T-REC-X.1051-202306-I/en