TECHNICAL CODE

INFORMATION AND NETWORK SECURITY - INCIDENT MANAGEMENT (FIRST REVISION)

Developed by

Malaysian Technical Standards Forum Bhd

Registered by

MCMC

Registered date: 4 April 2024

Development of technical codes

The Communications and Multimedia Act 1998 (Laws of Malaysia Act 588) ('the Act') provides for a Technical Standards Forum designated under section 184 of the Act or the Malaysian Communications and Multimedia Commission ('the Commission') to prepare a technical code. The technical code prepared pursuant to section 185 of the Act shall consist of, at least, the requirements for network interoperability and the promotion of safety of network facilities.

Section 96 of the Act also provides for the Commission to determine a technical code in accordance with section 55 of the Act if the technical code is not developed under an applicable provision of the Act and it is unlikely to be developed by the Technical Standards Forum within a reasonable time.

In exercise of the power conferred by section 184 of the Act, the Commission has designated the Malaysian Technical Standards Forum Bhd ('MTSFB') as a Technical Standards Forum which is obligated, among others, to prepare the technical code under section 185 of the Act.

A technical code prepared in accordance with section 185 shall not be effective until it is registered by the Commission pursuant to section 95 of the Act.

For further information on the technical code, please contact:

Malaysian Communications and Multimedia Commission (MCMC)
MCMC Tower 1
Jalan Impact
Cyber 6
63000 Cyberjaya
Selangor Darul Ehsan
MALAYSIA

Tel : +60 3 8688 8000
Fax : +60 3 8688 1000
Email : stpd@mcmc.gov.my
Website: www.mcmc.gov.my

OR

Malaysian Technical Standards Forum Bhd (MTSFB)
Level 3A, MCMC Tower 2
Jalan Impact
Cyber 6
63000 Cyberjaya
Selangor Darul Ehsan
MALAYSIA

Tel : +60 3 8680 9950
Fax : +60 3 8680 9940
Email : support@mtsfb.org.my
Website: www.mtsfb.org.my

Contents

Committee representation

This technical code was developed by Cybersecurity Management Sub Working Group which supervised by Security, Trust and Privacy Working Group under the Malaysian Technical Standards Forum Bhd (MTSFB) which consists of representatives from the following organisations:

Celcom Axiata Berhad

Deloitte Business Advisory Sdn Bhd

Digiforen (M) Sdn Bhd

FNS (M) Sdn Bhd

Maxis Broadband Sdn Bhd

TM Technology Services Sdn Bhd

Foreword

This technical code for Information and Network Security - Incident Management ('this Technical Code') was developed pursuant to section 185 of the Act 588 by the Malaysian Technical Standards Forum Bhd (MTSFB) via its Cybersecurity Management Sub Working Group.

This Technical Code is developed in reference to international standards such as ISO/IEC 27001:2022, ISO 27000, ISO 31000, NIST CSF, National Security Council - National Cyber Crisis Management - Response, Communication & Coordination Procedure.

Major modifications in this revision are as follows:

a) Addition of clause 2 on normative references.

b) Revision on the list of information security incidents to reflect on current cyber incidents to reflect on current cyber incidents or attack.

c) Revision on the information security incident management policy, handling an incident, post incident activities and information sharing.

d) Revision of annexes.

This Technical Code replaces the MCMC MTSFB TC G015:2018, Information and Network Security - Incident Management. The latter shall be deemed to be invalid to the extent of any conflict with this Technical Code.

This Technical Code shall continue to be valid and effective from the date of its registration until it is replaced or revoked.

INFORMATION AND NETWORK SECURITY - INCIDENT MANAGEMENT

0. Introduction

Incident management is a process used by Information Technology (IT) operation teams to respond and address unplanned events that can affect service quality or service operations. Incident management aims to identify and correct problems while maintaining normal service and minimizing impact to the business.

There are two main aims of the incident management process as follows.

a) To restore services back to normal operation as fast as possible as per agreed Service Level Agreement (SLA).

b) To mitigate the adverse effect of critical incidences on business operations.

This Technical Code describes the requirements for the management of network and information security incidents as illustrated in Figure 1.

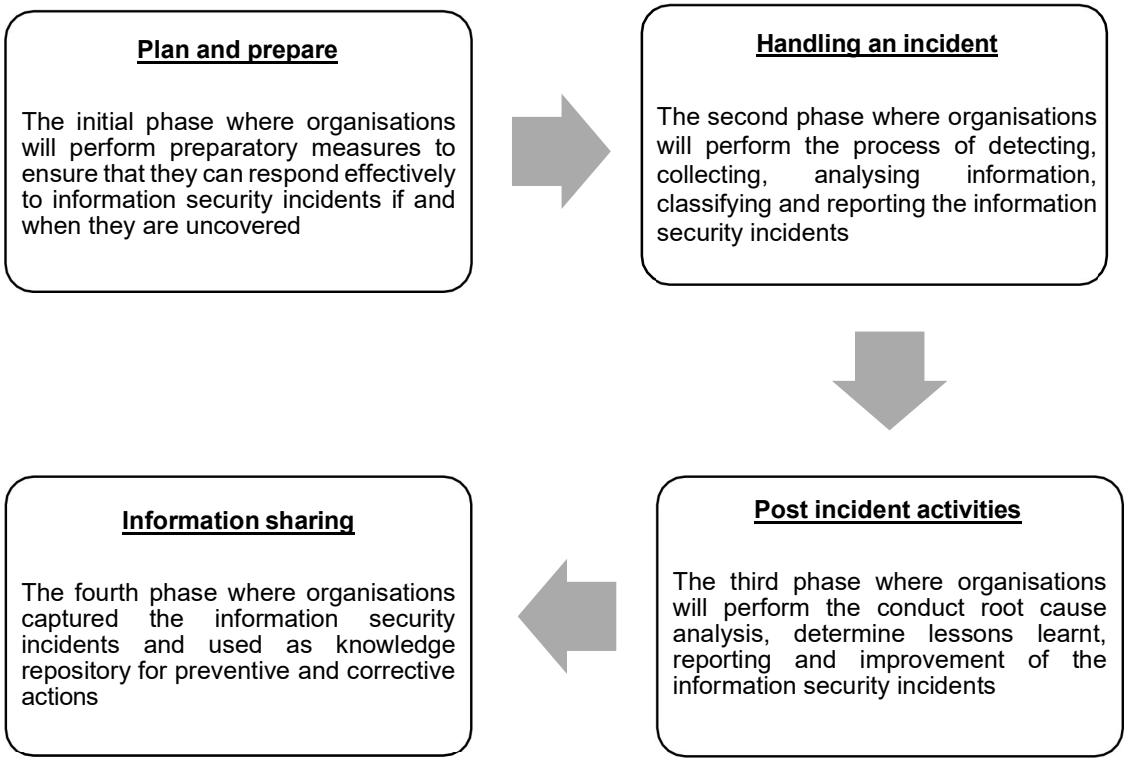

Figure 1. Components of information security incident management

1. Scope

This Technical Code specify requirements in managing information security incidents. This is to minimise the impact of security incidents to the organisations through a proper incident management process.

2. Normative references

The following normative references are indispensable for the application of this Technical Code. For dated references, only the edition cited applies. For undated references, the latest edition of the normative references (including any amendments) applies.

Incident Response Consortium, *Incident Response Playbook,*
https://www.incidentresponse.org/playbooks/

3. Terms and definitions

For the purposes of this Technical Code, the following terms and definitions apply.

3.1 Critical National Information Infrastructure (CNII)

Assets (physical and virtual), systems and functions that are vital to the nation that their incapacity or destruction would have a devastating impact on:

a) National economic strength

Confidence that the nation's key growth areas can successfully compete in the global market while maintaining favourable standards of living.

b) National image

Projection of national image towards enhancing stature and sphere of influence.

c) National defence and security

Guarantee sovereignty and independence whilst maintaining internal security.

d) Government capability to functions

Maintain order to perform and deliver minimum essential public services.

e) Public health and safety

Delivering and managing optimal healthcare to the citizen.

3.2 Incident management

The processes to detect, report, assess, contain, eradicate, recover and learn from information security incidents.

3.3 Incident response

Actions taken to mitigate or resolve an information security incident, including protecting and restoring normal operation conditions.

3.4 Incident Response Team (IRT)

A team of competent members of the organisation that handles information security incidents during the incident cycle. The team will analyse the incident data, determine impact and act appropriately to limit the damage and restore normal operational conditions.

3.5 Information security event

The identified occurrence of a system, service or network, indicating a possible breach of information security, policy or failures of control or a previously unknown situation that maybe security relevant.

3.6 Information security incident

Single or a series of unwanted or unexpected information security event that have a significant probability of compromising business operations and threatening information security. Below are the examples of the security incidents.

a) Denial of service.

b) Misuse of service, system and data or information.

c) Malicious code activity.

d) Violation of an explicit or implied information security policy.

e) Privilege abuse.

f) Phishing.

g) Credential leakage.

h) Data or Information leakage.

i) Unauthorised access.

4. Abbreviations

For the purpose of this Technical Code, the following abbreviations apply:

BAC	Board Audit Committee
BCM	Business Continuity Management
BISO	Business Information Security Officer
BoD	Board of Directors
CEO	Chief Executive Officer
CFO	Chief Financial Officer
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CNII	Critical National Information Infrastructure

COO	Chief Operating Officer
CSA	Certified SOC Analyst
DDoS	Distributed Denial of Service
DLP	Data Loss Prevention
ID	Identification
IDS	Intrusion Detection System
IaaS	Infrastructure as a Service
IP	Internet Protocol
IPS	Intrusion Prevention System
IRT	Incident Response Team
INS	Information and Network Security
IT	Information Technology
LEA	Law Enforcement Agency
MAC	Media Access Control
MTTD	Mean Time to Detect
MTTR	Mean Time to Response
NDA	Non-Disclosure Agreement
NSC	National Security Council
PaaS	Platform as a Service
PoC	Point of Contact
RCA	Root Cause Analysis
SaaS	Software as a Service
SIEM	Security Information and Event Management
SLA	Service Level Agreement
SME	Subject Matter Expert
SOC	Security Operations Centre
SOP	Standard Operating Procedures
SSL	Secure Sockets Layer
TISO	Technical Information Security Officer
TLP	Traffic Light Protocol
TLS	Transport Layer Security

5. Phase 1 - Plan and prepare

5.1 Information security incident management policy

The organisation shall establish an information security incident management policy as part of overall information security policy.

The key element of the policy may be individualised to the organisation, however, shall include but not limited to the following elements:

a) Statement of management commitment.

b) Purpose and objectives of the policy.

c) The scope of the policy.

d) Definition of information security incidents and related terms.

e) Organisational structure and definition of roles, responsibilities, and levels of authority shall include the following:

   i) Authority of the Incident Response Team (IRT) to confiscate or disconnect equipment and to monitor suspicious activity.

   ii) The requirements for reporting certain types of incidents.

   iii) The requirements and guidelines for external communications and information sharing (e.g. what can be shared with whom, when, and over what channels).

   iv) The handing over and an escalation in the incident management process.

f) Prioritisation or severity ratings of incidents.

g) Performance measures.

h) Reporting and incident closure.

An organisation shall ensure that its information security incident management policy is approved by authorise senior management. The policy shall be made available to every employee and contractor and should be addressed in information security awareness briefings and training.

5.2 Information security incident management plan

An organisation shall establish a security incident management plan, which includes, but not limited to the following elements:

a) Mission.

b) Strategies and goals.

c) Senior management approval.

d) Organisational approach to incident response.

e) Communications between internal and external party.

f) Metrics for measuring the incident response capability and its effectiveness.

g) Incident response capability improvement.

h) Lesson learnt.

The developed plan shall obtain management approval, be implemented and reviewed periodically to ensure the applicability and effectiveness in fulfilling goals for incident response.

5.3 Standard Operating Procedures (SOPs)

The organisation shall establish Standard Operating Procedures (SOPs) for types of information security events and incidents by addressing to the following elements:

a) Indicating groups or individual's (internal and external stakeholder) responsibility based on the information security incident management policy and plan.

b) The reporting process for the handling of event and incidents.

c) A pre-authorised delegation of decision making without normal approval process.

d) Management approval on change management in order to avoid any delay in response.

e) Align with the specific technical process, checklist and forms used by IRT.

An organisation shall conduct the following activities to ensure the accuracy and effectiveness of the SOPs:

a) Reviewed and validated.

b) Distribute to all team members.

c) Providing awareness, acculturation, and training for SOP users, where the SOP documents can be used as an instructional tool.

5.4 Incident Response Team (IRT) structure

The IRT is to provide the organisation with appropriate capability for assessing, responding to, and learning from information security events and incidents as well as providing the necessary coordination, management, feedback, and communication.

The establishment of the IRT should consider the following condition:

a) Appropriate for the size, structure, and the business nature of the organisation.

b) Evaluate if it requires a dedicated or ad hoc team.

c) Whenever justified, it is recommended to have the team lead and supported by the external party specialised in their respective domains.

d) Comprise of individuals from different parts of the organisation (e.g. business operations, information and communications technology, audit, human resources, and marketing).

e) Call tree list should be distributed and published by IRT members.

The responsibility of the IRT team lead shall include the following requirements:

a) To have a separate line of reporting to senior management, separate from normal business operations for critical information security incidents.

b) Authorised to make immediate decisions on incident management for a certain level of incident.

c) Ensure all IRT members are competent with required knowledge and skills levels.

Example of information security incident structure and an example of the roles and responsibilities that may be included in the IRT are shown in Annex A.

5.5 Communication with external party

The communications or public relations department shall report information security incidents to the appropriate authority, i.e., regulatory and law enforcement agencies and other relevant external parties, subject to senior management approval.

An organisation shall establish policies and procedures for coordination and release of information to the above parties. All contact and communication with the external party should be documented for liability and evidentiary purposes.

Organisations shall establish relationships between the IRT, and appropriate external interested parties as indicated in Figure 2.

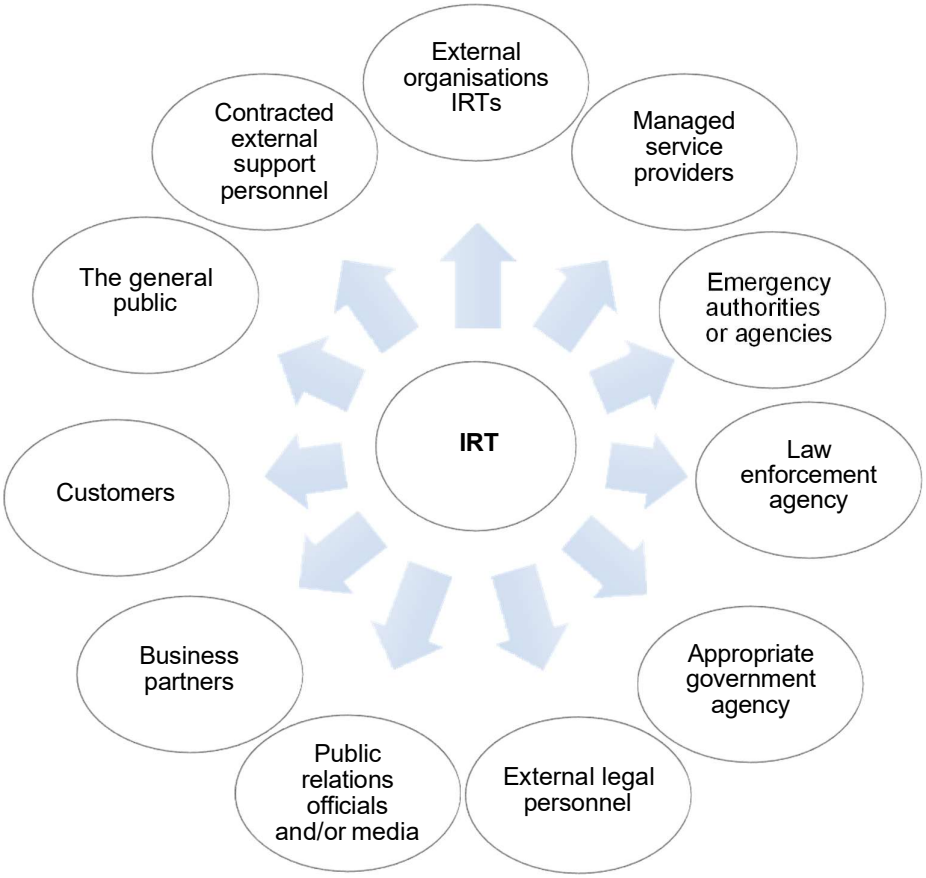

Figure 2. Relationships between the IRT and appropriate external interested parties

5.6 Awareness and training

An organisation shall ensure that the role of information security incident management is actively promoted as part of the corporate information security awareness and training program and include the following elements:

a) The implementation of the plan, including its scope and the security event, incident and vulnerability management workflow.

b) Reporting processes on information security events, incidents, and vulnerabilities.

c) Reservation of the incident information, and the output from the event, incident, or vulnerability database.

d) Controls on information confidentiality of sources.

e) SLAs and any constraints imposed by non-disclosure agreements.

f) Sharing the security incidents case study and lesson learned.

g) The authority and its reporting line of the organisation.

h) Audience and report distribution.

The training should be supported by specific exercises and testing for Point of Contact (PoC) and IRT members, as well as information security personnel and specific administrators to ensure its operability.

The information security incident awareness can be communicated through any means, e.g., workshops, websites, newsletters, posters, and stickers on monitors and laptops. The awareness program and related material shall be made available to all personnel, including new employees, third party users, and contractors, as relevant.

5.7 Exercise and testing

An organisation shall schedule a periodic test to assess the following.

a) To highlight potential flaws and problems that should arise during the management of information security events and incidents.

b) To check the operability and effectiveness of the processes or procedures.

c) To verify how the IRT responds to information security incidents, through the simulation of real incidents.

In the activities of the exercise and testing, an organisation shall ensure the following.

a) Creation of the simulated scenarios, based on real new information security threats.

b) Involve all the internal and external organisations in the management of information security incidents.

c) Ensure any changes made are tested and verified.

6. Phase 2 - Handling an incident

Handling of the incident on occurrences of information security events using the INS plan involves the process of detecting, analysing, containment, eradication, and recovery phase.

6.1 Resources in preparing to handle incidents

In ensuring timely and effective responses to information security incidents, the organisation shall obtain, prepare, and test all necessary technical and other support means, which may include the following:

a) Access to organisation's assets with an up-to-date asset register and information on their links to business functions.

b) Access to documented procedures related to crisis management.

c) Documented and disseminated communications processes.

d) The use of an information security event, incident or vulnerability database and the technical means to populate and update the database quickly, analyse its information and facilitate responses to information security incidents support the following:

   i) Quick acquisition of information security event, incident, or vulnerability reports.

   ii) Ensuring the collection of all data about the information system, service and/or network, and all data processed.

   iii) Facilitating the archiving and securing of collected information.

   iv) Enabling the preparation of printouts (e.g., of logs), including those showing the progress of an incident, and the resolution process and chain of custody.

   v) Recovery of the information system, service and/or network to normal operation.

e) Facilities for information security forensics evidence collection and analysis.

f) Adequate crisis management arrangements for the information security event, incident, or vulnerability database.

The pre-requisite requirement for handling incidents is shown in Annex B.

6.2 Incident detection

The organisation shall ensure the following activities are followed in the detection of information security event and incident:

a) To detect and report the occurrence of an information security event and incident, whether by one of the organisation's personnel/customers or automatically, aided by the following:

   i) Alerts generated by technical monitoring systems, such as Data Loss Prevention (DLP), Intrusion Detection System (IDS), antivirus software, and log analysers.

   ii) Alerts from monitoring systems such as firewalls, network flow analysis, web filtering and others such as from a threat intelligence and SIEM.

   iii) Anomalies detected by audits, investigations, or reviews.

iv) Suspicious events reported by third parties or regulators, trusted sources, subscription services.

b) To collect information on an information security event and incident. Users are to be informed that they shall:

i) Report all suspected information security weaknesses and breaches to a central point or helpdesk e.g., information failures, loss of services, detection of malicious code, denial of service attacks, errors from incomplete and inaccurate business data.

ii) Note all important details (e.g., type of weakness, breach, messages on the screen, details of unusual occurrences).

iii) Restrain from attempting to take remedial actions themselves.

c) To ensure all PoCs properly log all activities, results, and related decisions for later analysis. This can be done through the establishment of logging standards and procedures to ensure that adequate information is collected by logs and security software and that the data is reviewed regularly. To ensure effective logging, the organisation may take the necessary action as follows:

i) Configure systems to record the right events.

ii) Monitor these events effectively.

iii) Maintain sufficient historical data (as logs can be overwritten or have insufficient storage space)

iv) Make appropriate event logs available to investigators in a suitable format.

For incidents occurring in cloud environments, there are several key aspects of a cloud incident response system that differentiate it from a non-cloud incident response system, notably in the areas of governance, shared responsibility, and visibility, subject to cloud subscription model such as SaaS, Paas and IaaS. It is recommended for organisation to include in the agreement and SLA with cloud service provider on incident response management. The organisation may refer to Cloud Incident Response Framework from CSA.

The incident escalation process and turnaround time should be established with cloud service providers and periodically reviewed.

6.3 Incident analysis

Upon confirmation on the occurrence of an incident, the IRT shall immediately assess and validate each incident to determine its scope (i.e., which networks, systems, or applications are affected), its source and its cause to enable prioritisation of subsequent activities.

The following recommendations may be used as a guideline for making incident analysis easier and more effective:

a) Profiling of networks and systems; understand the normal manners of network, system and application to enable detection of the abnormal manner; such as detection and validation on anomaly/suspicious network, systems, apps, database activities or any suspected on social media incident violations.

b) Establish a log retention policy, that specifies the duration of time the log data shall be maintained for future analysis.

c) Correlating events among multiple indicator sources can be invaluable in validating whether a particular incident occurred.

d) Networks and systems clock synchronisation.

e) Deploy monitoring tools to monitor and analyse the specific traffic, performance and health.

An organisation shall develop or establish an Incident Response Playbook i.e ransomware, data breach/leakage, DDoS and phishing for detailed procedures in handling and responding to specific security incidents. Sample of Incident Response Playbook can be referred to Incident Response Consortium.

In the event of ransomware incident or any relevant incident, organisation should consider purchasing cyber insurance or incident negotiation service.

6.4 Preserving evidence

An organisation shall maintain a chain of evidence (custody) for both paper based and electronic information. A detailed written log of every action during the investigation shall be kept and at minimum to include the following:

a) Clear and precise evidence can be referred to for future reference including photos or images taken during incidents.

b) The sequence of events and actions taken can be reproduced when necessary.

This action log shall include, but not limited to the following:

a) Identifying information e.g. the location, serial number, model number, hostname, Media Access Control (MAC) addresses, and Internet Protocol (IP) addresses of a computer.

b) Name, title, and phone number of each individual who collected or handled the evidence during the investigation.

c) Time and date (including time zone) of each occurrence of evidence handling.

d) Locations where the evidence was stored.

All forensic investigation shall be performed on copies of the evidential material (e.g. using imaging technology) and the integrity of all evidential material shall be protected.

6.5 Incident documentation

All security incidents records shall be documented and tracked accordingly. This may be done by using an application or a database, such as an issue tracking system. This may help in ensuring that incidents are handled and resolved in a timely manner.

The issue tracking system should contain information on the following:

a) The present status of the incident new, in progress, forwarded for investigation, resolved i.e.

b) A summary of the incident.

c) Indicators related to the incident.

d) Other incidents related to this incident.

e) Actions were taken by all incident handlers on this incident.

f) Chain of custody, if applicable.

g) Impact assessments related to the incident.

h) Contact information for other involved parties (e.g. system owners, system administrators).

i) A list of evidence gathered during the incident investigation.

j) Comments from incident handlers.

k) Next steps to be taken (e.g. rebuild the host, upgrade an application).

The security incidents document or report shall be safeguarded to prevent from unauthorised access.

6.6 Incident triage (prioritisation)

Security incidents shall be prioritised and classified into severity levels based on the analyst's assessment of the impact of the attack. Table 1 may be referred for example of the severity levels kindly refer to Table 1. Organisational Cyber Impact Assessment Matrix in Annex E.

6.7 Incident notification

When an incident is analysed and prioritised, the IRT shall notify the appropriate individuals so that all responsible parties involved will play their roles.

Information security incident management policy shall include provisions concerning incident reporting, e.g., initial notification, regular status updates.

The reporting requirements may vary among organisations, but parties that are typically notified include:

a) Chief Information Officer (CIO) or senior management.

b) Head of information security.

c) Local information security officer or designated CISO, TISO, or BISO

d) Other IRT within the organisation.

e) External IRT (if appropriate).

f) System owner/business user.

g) Human resources (for cases involving employees, such as harassment through email).

h) Corporate communication (for incidents that may generate publicity).

i) Legal department (for incidents with potential legal ramifications).

j) Regulatory.

k) Law enforcement (if appropriate).

6.8 Incident containment

Actions to be taken after the initial investigation (and often as part of that investigation) is to contain the damage by the information security incident, for example by stopping it from spreading to other networks and devices.

In general, containment comprises a number of concurrent actions aimed at reducing the immediate impact of the information security incident with an objective to restore or resume to normal operational conditions.

Mechanism or approach to containing the information security incident may include the following but not limited to:

a) Network blocking and isolation.

b) Blocking malware or malicious sources e.g. email addresses and websites.

c) Closing particular ports and mail servers.

d) Disabled relevant access.

e) Isolating systems.

f) Disconnect affected systems.

g) Resetting credentials.

An organisation shall consider creating separate containment strategies for different types of major information security attack, with criteria documented clearly to facilitate decision making.

These criteria may include evaluating the:

a) Potential damage to and theft of resources.

b) Need for evidence preservation.

c) Service availability e.g., network connectivity, services provided to an external party.

d) Time and resources needed to implement the strategy.

e) The effectiveness of the strategy e.g., partial containment, full containment.

f) Duration of the solution (e.g., emergency workaround to be removed in 4 h, a temporary workaround to be removed in two weeks, permanent solution).

6.9 Incident cause eradication

Effective eradication plans shall be executed timely and precisely to prevent an attacker from re-establish new attack. Eradication is often required to eliminate key components of the incident e.g., removing the attack from the network, deleting malware and disabling breached user accounts, as well as identifying and mitigating vulnerabilities that were exploited.

Action to be taken during the eradication process may include the following:

a) Identifying all affected hosts.

b) Perform further analysis.

c) Develop a response (preferably in advance) if the attacker uses a different method of attack.

d) Monitor the response from the attacker.

6.10 Recovery

The final step in responding to an information security incident is to restore systems to normal operation, confirm that the systems are functioning normally, and remediate vulnerabilities to prevent similar incidents occurring.

An appropriate recovery plan shall be established, which may include the following:

a) Restore from last cleaned backup or sources.

b) Rebuilding infected systems (often from known 'clean' sources).

c) Replacing compromised files with clean versions.

d) Removing temporary constraints imposed during the containment period.

e) Reconfigure system settings i.e., by changing passwords and hardening network perimeter security, such as firewall rulesets.

f) Testing systems thoroughly, including security controls and functionalities.

g) Confirming the integrity of business systems and controls.

h) Any other detailed activity or steps defined in the respective incident playbook.

Upon remediation, an independent vulnerability or penetration testing or compromise assessment of the affected systems should be considered to validate the security gaps has been remediated.

Relevant stakeholders shall be informed accordingly and be reported that recovery was completed successfully and note any exceptions and other significant findings.

7. Phase 3 - Post incident activities

7.1 Lessons learn

The organisation shall establish an action plan explaining activity taken to leverage lessons learned from the incident and to become more resilient in the face of future information security attacks. The action plan should include projects or initiatives, technical and non-technical, that will help reduce an attacker's chance of success and respond to an attacker's activities more rapidly and effectively.

A post-mortem to discuss the lesson learned from the incident shall be held and the questions to use as a guidance to understand the problems may be referred in Annex C.

Lesson learned and Root Cause Analysis (RCA) may be valuable for the following:

a) Improve the training and material contents to enhance current skills.

b) Improving incident response policies and procedures, guidelines and playbook.

c) Continuously monitor action items to track the progress until the closure.

d) Total hours of involvement and the cost may be used to justify additional funding of the IRT.

e) Incident characteristics may indicate systemic security weaknesses and threats, as well as changes in incident trends. This data can be put back into the risk assessment process, ultimately leading to the selection and implementation of additional controls; Update risk register, review and improve security controls to prevent recurrence of similar incidents.

f) To measure the key performance indicator for incident response activities (i.e. MTTD, MTTR).

7.2 Using collected incident data

Organisations shall decide what incident data to collect based on reporting requirements and develop possible metrics that may include incident related data as follows:

a) Number of incidents handled

The number of incidents handled is best taken as a measure of the relative amount of work that the IRT had to perform, not as a measure of the quality of the team unless it is considered in the context of other measures that collectively give an indication of work quality. It is more effective to produce separate incident counts for each incident category.

b) Time per incident

For each incident, time should be measured in several ways:

i) The total amount of time spent working on the incident.

ii) Elapsed time from the beginning of the incident-to-incident discovery to the initial impact assessment, and to each stage of the incident handling process e.g., containment, recovery.

iii) Time is taken by IRT to respond to the initial report of the incident.

iv) Time is taken to report the incident to management and, if necessary, appropriate external entities.

c) Objective assessment of each incident

The response to an incident that has been resolved can be analysed to determine its effectiveness. Following are examples of performing an objective assessment of an incident:

i) Determining if the actual cause of the incident was identified, and identifying the vector of attack, the vulnerabilities exploited, and the characteristics of the targeted or victimised systems, networks, and application.

ii) Reviewing logs, forms, reports, and other incident documentation for adherence to established incident response policies and procedures.

iii) Identifying which precursors and indicators of the incident were recorded to determine how effectively the incident was logged and identified.

iv) Determining if the incident caused damage before it was detected.

v) Determining if the incident is a recurrence of a previous incident.

vi) Calculating the estimated monetary damage from the incident e.g. information and critical business processes negatively affected by the incident.

vii) Measuring the difference between the initial impact assessment and the final impact assessment.

viii) Identifying which measures, if any, could have prevented the incident.

d) Determine if the incident was handled efficiently and if the outcome was satisfactory.

7.3 Evidence retention

Organisations shall establish policy for how long evidence from an incident should be retained as per applicable laws and regulations requirements. The following factors shall be considered during the policy creation:

a) Legal obligation

Evidence may need to be retained to be used for legal and litigation matters in ensuring evidence is admissible in court.

b) Data retention

Organisations shall have data retention policies that define the duration of certain types of data shall be kept.

7.4 Report incident to relevant stakeholders

Formal reporting shall be established once an information-security incident has been successfully closed.

The report shall include the following:

a) A full description of the nature of the incident, its chronology, causes and actions taken to recover.

b) A realistic estimate of the financial loss of the incident, as well as other impacts on the business, such as reputation damage, potential revenue loss or service impact.

c) Recommendations on enhancement, additional controls or alternative solutions required to prevent, detect, remediate, or recover from information security incidents more effectively.

7.5 Cyber simulation or drills

Cyber drill exercise is defined as an activity to simulate information security incident in various scenario. The objective of cyber simulation is to gauge organisation's incident response team competency, capability, familiarisation with process and the response time to detect and recover on realistic scenario among others:

a) To upskills cyber response team.

b) To improve capability.

c) To embrace teamwork.

d) To familiarise with relevant tools and understand different types of incidents.

Organisation shall conduct cyber simulation exercises such as call tree exercise, tabletop exercise, controlled environment cyber drill and phishing simulation campaign regularly or at minimum once a year or annually to enhance cyber resilience.

8. Phase 4 - Information sharing

Coordinating and sharing information with partner organisations may strengthen an organisation's ability to effectively respond to information security incidents.

8.1 Sharing information with external party

Prior to reaching out for assistance or reporting to an external party, it is critical that an organisation understand both obligations for reporting and requirements for protecting sensitive information.

Key information sharing planning considerations shall include the following:

a) The purpose of the information sharing.

b) The content of information to be shared or at what level of detail.

c) The parties to share information with.

d) The point to initiate the sharing.

e) The method of sharing and the protections required.

An organisation should consider using a Traffic Light Protocol (TLP) for information dissemination and sharing. Details of TLP can referred in Annex F.

8.2 Sharing agreements and breach reporting requirements

Information sharing shall be driven by a combination of concerns regarding voluntary permissive sharing to achieve organisational objectives, and mandatory notification guided by regulation or legal obligations.

An organisation intent to report or share information with external party such as regulators and Law Enforcement Agency (LEA) which include the following activities:

a) Consult with the legal department before initiating any coordinated efforts.

b) Seek endorsement from internal committee for sharing information to external party.

c) There may be contracts or other agreements that need to be established before discussions occur, (i.e., is a Non-Disclosure Agreement (NDA) to protect the confidentiality of the organisation's most sensitive information).

d) Consider any existing regulatory requirements for reporting to relevant regulatory bodies.

8.3 Information sharing methods

Information may be shared in a variety of ways depending on the objectives. An organisation shall consider the parties to share the information and the nature of the approach. Information sharing techniques may include but not limited to:

a) Authorised person to person.

b) Electronic data transfer via the secured channel.

c) Standard information sharing template acceptable by both parties.

Annex A
(Informative)

Example of the roles and responsibilities

The example of the roles and responsibilities that may be included in the IRT are shown in Table A.1 and example of the information security incident structure are illustrated in Figure A.1.

Table A.1. Example of the roles and responsibilities that may be included in the IRT

Domain	IRT members	IRT manager	Senior management	End-users	Legal team	Communications or public relations department	Facility/physical security officer	BCM manager
Incident management Manage the information security event and incident from the moment of its detection until its closure.	R	A	C	I				
Business decision capability a) Assess the business impact and address the need for a solution to resolve the incident. b) Engage the right resources. c) Take decisions on the appropriate action to be taken.	R	A	C	I				
Network management capabilities a) Technical experts on the organisation's network (firewall, proxies, Intrusion Prevention System (IPS), routers, switches, etc.). b) Analyse, block or restrict the data flow in and out of your network. c) IT operations information security and business continuity.	R	A	C	I				
Workstation and server administrator capabilities (admin rights) Analyse and manage compromised workstations and servers.	R	A	C	I				

Table A.1. Example of the roles and responsibilities that may be included in the IRT *(continued)*

Domain	IRT members	IRT manager	Senior management	End-users	Legal team	Communications or public relations department	Facility/physical security officer	BCM manager
Forensic investigation Gather and analyse evidence in an appropriate way i.e., in a way that the evidence is acceptable by a court of law.	R	A	C	I				
Legal advice a) Assess the contractual and judicial impact of an incident. b) Guarantee that incident response activities stay within legal, regulatory and the organisation's policy boundaries. c) Filing a complaint.	I	A	C		R			
Communication management a) Communicate in an appropriate way to all concerned stakeholder groups. b) Answer customer, shareholders, press questions right away.	I	A	C			R		
Physical security a) Handle the aspects of the incident that are linked to physical security. b) The physical access to the premises. The physical protection of the information security infrastructure.	I	A	C				R	
Crisis management Handle required activities upon BCM activation.	I	A	C					R
Note: R is responsible, A is accountable, C is consulted, and I is informed.								

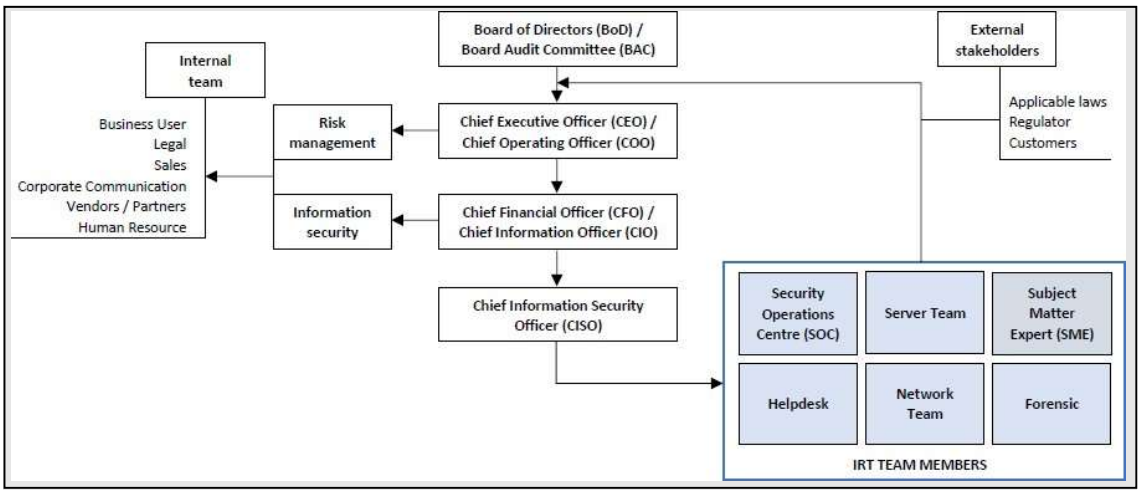

Figure A.1. Example of an information security incident structure

Annex B
(Informative)

Pre-requisite requirement for handling incidents

B.1. Obtain tools and resources that may be of value during incident handling

The IRT will be more efficient at handling incidents if various tools and resources are already available to them. Examples include contact lists, encryption software, network diagrams, backup devices, digital forensic software, and port lists.

B.2. Prevent incidents from occurring by ensuring that networks, systems, and applications are sufficiently secure

Preventing incidents is beneficial to the organisation and reduces the workload of the IRT. Performing periodic risk assessments and reducing the identified risks to an acceptable level is effective in reducing the number of incidents. Awareness of security policies and procedures by users, IT staff, and management is also very important.

B.3. Identify precursors and indicators through alerts generated by several types of security software

Intrusion detection and prevention systems, antivirus software, and file integrity checking software are valuable for detecting signs of incidents. Each type of software may detect incidents that the other types of software cannot, so the use of several types of computer security software is highly recommended. Third party monitoring services can also be helpful.

B.4. Establish mechanisms for external party to report incidents

An external party may want to report incidents to the organisation; for example, they may believe that one of the organisation's users is attacking them. Organisations should publish a phone number and email address that external party can use to report such incidents.

B.5. Require a baseline level of logging and auditing on all systems, and a higher baseline level on all critical systems

Logs from operating systems, services, and applications frequently provide value during incident analysis, particularly if auditing was enabled. The logs can provide information such as which accounts were accessed and what actions were performed.

B.6. Profile networks and systems

Profiling measures the characteristics of expected activity levels so that changes in patterns can be more easily identified. If the profiling process is automated, deviations from expected activity levels can be detected and reported to administrators quickly, leading to faster detection of incidents and operational issues.

B.7. Understand the normal behaviours of networks, systems, and applications

Team members who understand normal behaviour shall be able to recognise abnormal behaviour more easily. This knowledge can best be gained by reviewing log entries and security alerts; the handlers should become familiar with the typical data and can investigate the unusual entries to gain more knowledge.

B.8. Create a log retention policy

Information regarding an incident may be recorded in several places. Creating and implementing a log retention policy that specifies how long log data should be maintained may be extremely helpful in the analysis because older log entries may show inspection activity or previous instances of similar attacks.

B.9. Perform event correlation

Evidence of an incident may be captured in several logs. Correlating events among multiple sources can be invaluable in collecting all the available information for an incident and validating whether the incident occurred.

B.10. Keep all host clocks synchronised

If the devices reporting events have inconsistent clock settings, event correlation will be more complicated. Clock inconsistencies may also cause issues from an evidentiary standpoint.

B.11. Maintain and use a knowledge base of information

Handlers need to reference information quickly during incident analysis; a centralised knowledge base provides a consistent, maintainable source of information. The knowledge base should include general information, such as data on precursors and indicators of previous incidents.

B.12. Start recording all information as soon as the team suspects that an incident has occurred

Every step is taken, from the time the incident was detected to its final resolution, shall be documented and timestamped. Information of this nature can serve as evidence in a court of law if the legal prosecution is pursued. Recording the steps performed can also lead to a more efficient, systematic, and less error-prone handling of the problem.

B.13. Safeguard incident data

It often contains sensitive information regarding such things as vulnerabilities, security breaches, and users that may have performed inappropriate actions. The team shall ensure that access to incident data is restricted properly, both logically and physically.

B.14. Prioritise handling of the incidents based on the relevant factors

Because of resource limitations, incidents should not be handled on a first come, first served basis. Instead, organisations should establish written guidelines that outline how quickly the IRT shall respond to the incident and what actions should be performed, based on relevant factors such as the functional and information impact of the incident, and the likely recoverability from the incident.

This saves time for the incident handlers and provides a justification to management and system owners for their actions. Organisations should also establish an escalation process for those instances when the team does not respond to an incident within the designated time.

B.15. Include provisions regarding incident reporting in the organisation's incident response policy

An organisation should specify which incidents shall be reported, when they shall be reported, and to whom. The parties most commonly notified are the CIO, head of information security, local information security officer, other IRT within the organisation, and system owners.

B.16. Establish strategies and procedures for containing incidents

It is important to contain incidents quickly and effectively to limit their business impact. An organisation should define acceptable risks in containing incidents and develop strategies and procedures accordingly. Containment strategies should vary based on the type of incident.

B.17. Follow established procedures for evidence gathering and handling

The IRT should clearly document how all evidence has been preserved. Evidence should be accounted for at all times. The IRT should meet with legal staff and law enforcement agencies to discuss evidence handling, then develop procedures based on those discussions.

B.18. Capture volatile data from systems as evidence

This includes lists of network connections, processes, login sessions, open files, network interface configurations, and the contents of memory. Running carefully chosen commands from trusted media can collect the necessary information without damaging the system's evidence.

B.19. Obtain system snapshots through full forensic disk images, not file system backups

Disk images should be made to sanitised write protectable or write once media. This process is superior to a file system backup for investigatory and evidentiary purposes. Imaging is also valuable in that it is much safer to analyse an image than it is to perform analysis on the original system because the analysis may inadvertently alter the original.

B.20. Hold lessons learned meetings after major incidents

Lessons learned meetings are extremely helpful in improving security measures and the incident handling process itself.

Annex C
(Informative)

Questions to use as a guidance to understand the incidents

The following are questions to use as a guidance for the incidents:

a) Has the root cause of the incident identified?

b) Has the gap analysis conducted?

c) How effective the incident management process?

d) Were the documented procedures followed?

e) Were they adequate?

f) What information was needed sooner?

g) Were any steps or actions taken that might have inhibited the recovery?

h) What would the staff and management do differently the next time a similar incident occurs?

i) How could information sharing with other organisations have been improved?

j) What can corrective actions prevent similar incidents in the future?

k) What precursors or indicators should be watched for in the future to detect similar incidents?

l) What additional tools or resources are needed to detect, analyse, and mitigate future incidents?

Annex D
(Informative)

Recommended list of training and certifications

Recommended but not limited list of training and certifications on cyber security:

a) ISC2 Certified Cloud Security Professional (CCSP)

b) CSA Certified of Cloud Security Knowledge (CCSK)

c) COMPTIA Cloud+

d) GIAC Public Cloud Security (GPCS) for AWS, GCP & Azure

e) GIAC Cloud Security Automation (GCSA)

f) EC-Council Certified Cloud Security Engineer (CCSE)

g) GIAC Certified Incident Handler (GCIH)

h) EC-Council Incident Handler (ECIH)

i) EC-Council Certified SOC Analyst (CSA)

j) GIAC Reverse Engineering Malware (GREM)

k) EC-Council Certified Threat Intelligence Analyst (CTIA)

l) GIAC Cyber Threat Intelligence (GCTI)

m) Computer Hacking Forensic Investigator (CHFI)

n) GIAC Certified Forensic Analyst (GCFA)

o) GIAC Reverse Engineering Malware (GREM)

p) GIAC Cloud Forensics Responder (GCFR)

q) GIAC Certified Forensic Examiner (GCFE)

r) GIAC Advanced Smartphone Forensics (GASF)

s) GIAC Network Forensic Analyst (GNFA)

t) GIAC Law of Data Security & Investigations (GLEG)

u) GIAC iOS and macOS Examiner (GIME)

v) Certified Information Systems Security Professional (CISSP)

w) Certified Incident Handling Engineer (CIHE)

x) Certified Information Security Manager (CISM)

y) Certified Information Systems Auditor (CISA)

z) GIAC Certified Incident Handler (GCIH)

aa) CyberSec First Responder: Threat Detection and Response (CFR)

bb) Certified Cyber Security Incident Handler (CCSIH)

cc) Certified SOC Analyst (CSA)

dd) IBM Certified SOC Analyst

ee) SANS SEC540: Cloud Security and DevOps Automation

Annex E
(Informative)

Organisational cyber impact assessment matrix

Table E.1. Organisational Cyber Impact Assessment Matrix

Impact level	Areas of impact				
	System downtime and business operation	**Financial damage**	**Corporate image or reputation damage**	**Health and safety**	**Personal data violation**
Insignificant	(i) No impact on critical systems and services; and/or (ii) Critical services downtime is within Service Level Agreement (SLA) requirement.	(i) No loss of gross daily revenue; and/or (ii) No loss of productivity	(i) No negative publicity to corporate image or reputation and issues were not made known to management.	(i) No staff and/or public affected	(i) None
Minor	(i) Less than or equal to 5 % of critical services degradation ≤ 5 % of critical services degradation); and/or; (ii) Less than or equal to 1 hour critical services downtime after expiration of SLA ≤ 1 hour critical services downtime after expiration of SLA)	(i) Less than or equal to 2 % of daily revenue (2 % ≤ daily revenue); and/or (ii) Less than or equal to 10% loss of productivity per day; and/or (iii) Less than the cost to fix the vulnerability.	(i) No negative publicity to corporate image or reputation but issues were officially made known to management; and/or (ii) Minimal damage	(i) Less than 1 % of staff affected within organisation; and/or (ii) At least one report of a member of the public is affected.	(i) One Personally Identifiable Information disclosed.

Medium	(i) More than 5 % and less or equal to 10 % of critical services degradation (5 % < critical services degradation ≤ 10 %); and/or (ii) More than or equal to 1 - 3 hours critical services downtime (1 hour < critical services downtime ≤ 3 hours) after expiration of SLA.	(i) More than 2 % and less or equal to 5 % of daily revenue (2 % > daily revenue ≤ 5 %); and/or (ii) Less than or equal to 30 % loss of productivity per day; and/or (iii) Minor effect on annual profit.	(i) Issues were discussed in blogs and online social network that affect corporate image/reputation; and/or (ii) Loss of major accounts.	(i) Between 1-5 % of staff affected within organisation; and/or (ii) Report of localized area where public is affected.	(i) Hundreds of PII disclosed
Major	(i) More than 11 % and less or equal to 15 % of critical services degradation (11 % < critical services degradation ≤ 15 %); and/or (ii) More than or equal to 4 - 5 hours critical services downtime (4 hours ≤ critical services downtime ≤ 5 hours) after expiration of SLA.	(i) More than 5 % and less or equal to 10 % of daily revenue (5 % > daily revenue ≤ 10 %); and/or (ii) Less than or equal to 50 % loss of productivity per day; and/or (iii) Significant effect on annual profit.	(i) Issues were discussed in all mediums of communications locally that affect corporate image or reputation; and/or (ii) Loss of goodwill.	(i) Between 6 % - 10 % of staff affected within organisation; and/or (ii) Multiple localised area where public is affected.	(i) Thousands of PII disclosed.
Critical	(i) More than 15 % critical services degradation (15 % > critical services degradation); and/or (ii) More than 5 hours critical system downtime (5 hours < critical system downtime) after expiration of SLA.	(i) More than 10 % loss of daily revenue (10 % > daily revenue); and/or (ii) More than 50 % loss of productivity per day; and/or (iii) Bankruptcy	(i) Issues were discussed in all mediums of communications locally and internationally that affect corporate image or reputation; and/or (ii) Brand damage.	(i) More than 10 % of staff affected within organisation; and/or (ii) Mass public is affected.	(i) Millions of PII disclosed.

Annex F
(Informative)

Traffic Light Protocol (TLP)

Table F.1. Type and definitions of Traffic Light Protocol (TLP)

Type of TLP	Definitions
TLP: red	Not for disclosure restricted to participants only
TLP: amber + strict	Limited disclosure, restricted to participants' organisation.
TLP: amber	Limited disclosure, restricted to participants' organisation and its clients (see terminology definitions).
TLP: green	Limited disclosure, restricted to the community
TLP: clear	Disclosure is not limited

TLP usage

F.1. TLP: red

When should it be used? Sources may use TLP: red when information cannot be effectively acted upon without significant risk for the privacy, reputation, or operations of the organisations involved. For the eyes and ears of individual recipients only, no further.

How should it be shared? Recipients may not share TLP: red information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP: red information is limited to those present at the meeting. In most circumstances, TLP: red should be exchanged verbally or in person.

F.2. TLP: amber + strict

When should it be used? Sources may use TLP: amber + strict when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organisation.

How should it be shared? Recipients may share TLP: amber + strict information only with members of their own organisation on a need-to-know basis to protect their organisation and prevent further harm.

F.3. TLP: amber

When should it be used? Sources may use TLP: amber when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organisations involved. Note that TLP: amber + strict should be used to restrict sharing to the recipient organisation only.

How should it be shared? Recipients may share TLP: amber information with members of their own organisation and its clients on a need-to-know basis to protect their organisation and its clients and prevent further harm.

F.4. TLP: green

When should it be used? Sources may use TLP: green when information is useful to increase awareness within their wider community.

How should it be shared? Recipients may share TLP: green information with peers and partner organisations within their community, but not via publicly accessible channels. Unless otherwise

specified, TLP: green information may not be shared outside of the cybersecurity or cyber defense community.

F.5. TLP: clear

When should it be used? Sources may use TLP: clear when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.

How should it be shared? Recipients may share this information without restriction. Information is subject to standard copyright rules.

Bibliography

[1] ISO/IEC 27035, *Information technology - Security techniques - Information security incident management*

[2] ISO27001:2022, *Information security - cybersecurity and privacy protection - Information security management systems - Requirements*

[3] ISO27002:2022, *Information security - cybersecurity and privacy protection - Information security controls*

[4] CISA*, Cybersecurity & Infrastructure Security Agency Traffic Light Protocol*

[5] *Incident Response Playbook, https://www.incidentresponse.org/playbooks*

[6] NCCM, *National Cyber Crisis Management Response, Communication & Coordination Procedure - Organisational Cyber Impact Assessment Matrix*

[7] CREST, *Cyber Security Incident Response Guide*

[8] ISACA, *Incident Management and Response*

[9] MCMC Network Security Centre Standard Operating Procedure

[10] NIST 800-61 Revision 2, *Computer Security Incident Handling Guide*

[11] *Cloud Security Alliance, https://cloudsecurityalliance.org/artifacts/cloud-incident-response-framework-a-quick-guide/*

[12] *SANS Incident Response Cycle, https://resource.redcanary.com/rs/003-YRU-314/images/Red%20Canary_%20IR%20RACI%20Matrix%20Template.xlsx*

Acknowledgements

Members of the Cybersecurity Management Sub Working Group

Mr Azlan Mohamed Ghazali (Chair/Draft Lead)	Deloitte Business Advisory Sdn Bhd
Mr Mohd Fairuz Ismail (Vice Chair)	Deloitte Business Advisory Sdn Bhd
Mr Khairul Ekhwan Kamarudin (Secretariat)	Malaysian Technical Standards Forum Bhd
Mr Zaime Kharis Zainuddin	Celcom Axiata Berhad
Mr Ong Yew Seng	Digiforen (M) Sdn Bhd
Mr Mohd Wafiuddin Ali	FNS (M) Sdn Bhd
Mr Khairudin Pie	Maxis Broadband Sdn Bhd
Mr Khairul Hadi Shaari	TM Technology Services Sdn Bhd

By invitation:

Ms Norahana Salimin	Bank Muamalat Malaysia Berhad
Mr Morshidi Mostapa	Bank Negara Malaysia
Mr Kilausuria Abdullah	Cybersecurity Malaysia