TECHNICAL CODE

INFORMATION AND NETWORK SECURITY - INCIDENT MANAGEMENT

Developed by

Malaysian Technical Standards Forum Bhd

Registered by

Registered date:

15 October 2018

MCMC MTSFB TC G015:2018

Development of technical codes

The Communications and Multimedia Act 1998 ('the Act') provides for 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 requirement 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
http://www.skmm.gov.my

OR

Malaysian Technical Standards Forum Bhd (MTSFB)
Malaysian Communications & Multimedia Commission (MCMC)
Off Persiaran Multimedia
Jalan Impact
Cyber 6
63000 Cyberjaya
Selangor Darul Ehsan
MALAYSIA

Tel: +60 3 8320 0300
Fax: +60 3 8322 0115
http://www.mtsfb.org.my

Contents

Page

Committee representation iii
Foreword iv

0. Introduction 1
1. Scope 2
2. Terms and definitions 2
   2.1 Critical National Information Infrastructure (CNII) 2
   2.2 Incident management 2
   2.3 Incident response 2
   2.4 Incident Response Team (IRT) 2
   2.5 Information security event 3
   2.6 Information security incident 3
3. Abbreviations 3
4. Plan and prepare (phase 1) 4
   4.1 Information security incident management policy 4
   4.2 Information security incident management plan 5
   4.3 Standard Operating Procedures (SOPs) 5
   4.4 Incident Response Team (IRT) structure 6
   4.5 Communication with external party 6
   4.6 Awareness and training 7
   4.7 Exercise and testing 8
5. Handling an incident (phase 2) 8
   5.1 Resources in preparing to handle incidents 8
   5.2 Incident detection 9
   5.3 Incident analysis 10
   5.4 Incident documentation 10
   5.5 Incident prioritisation 11
   5.6 Incident notification 12
   5.7 Incident containment 12
   5.8 Incident cause eradication 13
   5.9 Gathering and preserving evidence 13
   5.10 Recovery 14
6. Post incident activities (phase 3) 14
   6.1 Lessons learned 14
   6.2 Using collected incident data 15

6.3 Evidence retention 16
6.4 Report incident to relevant stakeholders....16
6.5 Other improvements....16
7. Information sharing (phase 4) 16
7.1 Sharing information with external party....17
7.2 Sharing agreements and breach reporting requirements 17
7.3 Information sharing methods 17

Annex A Example of the roles and responsibilities 18
Annex B Pre-requisite requirement for handling incidents....21
Annex C Questions to use as a guidance to understand the incidents....24
Bibliography 25

Committee representation

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

Al Hijrah Media Corporation

Basis Bay Malaysia

Celcom Axiata Berhad

Malaysia Digital Economy Corporation Sdn Bhd

Maxis Communications Berhad

MEASAT Broadcast Network Sdn Bhd

MYTV Broadcasting Sdn Bhd

Provintell Technologies Sdn Bhd

Telekom Applied Business Sdn Bhd

Telekom Malaysia Berhad

TIME dotCom Berhad

Universiti Kuala Lumpur

Universiti Tenaga Nasional

webe digital 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 Application Security Sub Working Group.

This Technical Code shall continue to be valid and effective until reviewed or cancelled.

INFORMATION AND NETWORK SECURITY - INCIDENT MANAGEMENT

0. Introduction

Communication networks and information systems have become an essential factor in economic and social development, whereby computing and networking are now utilities in the same way as electricity and water supplies. Therefore, the security of communication networks and information systems, and particularly their availability, is of increasing concern to society.

Incident management is all about getting a handle on Information Technology (IT) service management problems. Successful incident management will prevent these problems from interrupting business processes (any longer than necessary) or affecting other IT services.

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)s; and

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.

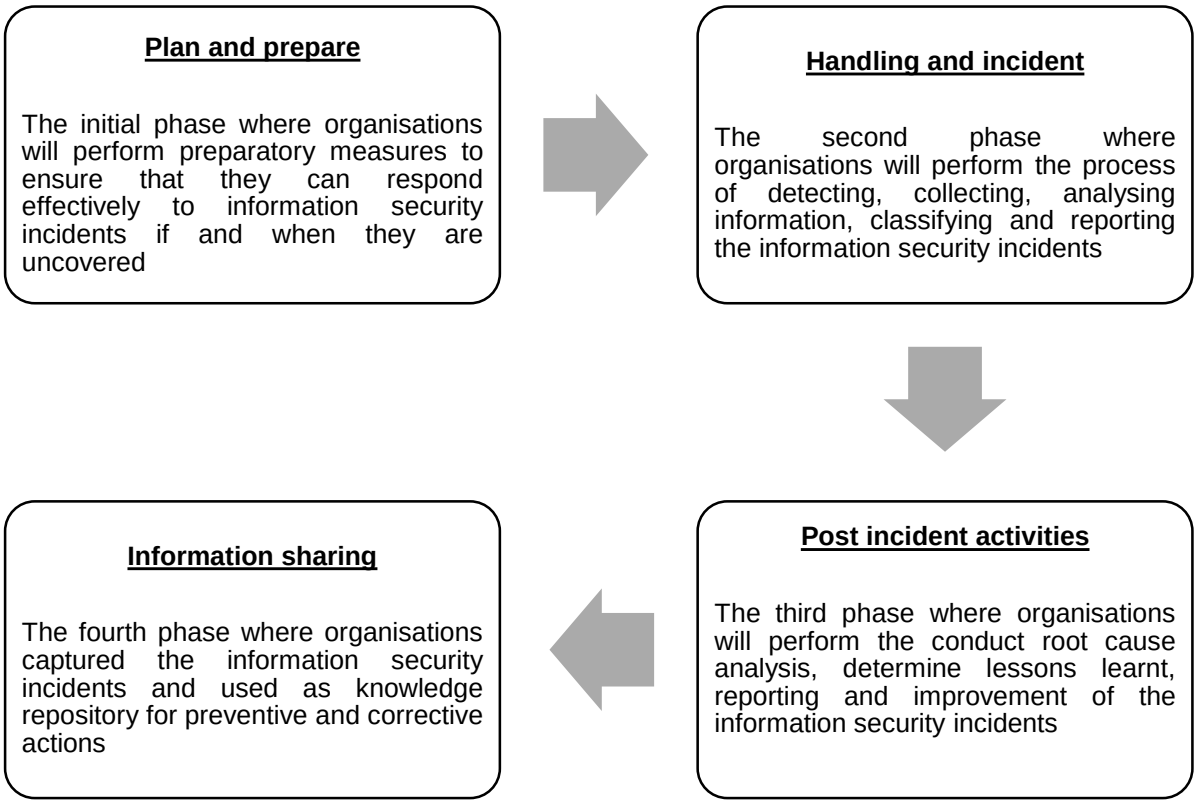

Figure 1. Component of information security incident management

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. Terms and definitions

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

2.1 Critical National Information Infrastructure (CNII)

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

a) National economic strength

Confidence that the nation's key growth area 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 health care to the citizen.

2.2 Incident management

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

2.3 Incident response

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

2.4 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.

2.5 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.

2.6 Information security incident

Single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security for example:

a) loss of confidentiality of data/information;

b) compromise of the integrity of data/information;

c) unwanted denial of service;

d) misuse of service, system and data/information;

e) physical damage to the system;

f) virus/worm outbreaks;

g) violation of an explicit or implied security policy;

h) unauthorised use of a system for the processing or storage of data; and

i) unauthorised changes to system baseline, hardware, firmware, or software characteristics and etc.

3. Abbreviations

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

BAC	Board Audit Committee
BCM	Business Continuity Management
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
DDoS	Distributed Denial of Service
DLP	Data Loss Prevention
ID	Identification
IDS	Intrusion Detection System
IP	Internet Protocol
IPS	Intrusion Prevention System

IRT	Incident Response Team
IT	Information Technology
MAC	Media Access Control
NDA	Non-Disclosure Agreement
NSC	National Security Council
POC	Point of Contact
SLA	Service Level Agreement
SME	Subject Matter Expert
SOC	Security Operations Centre
SOP	Standard Operating Procedures
SSL	Secure Sockets Layer
TLS	Transport Layer Security
X-MAYA	National Cyber Crisis Exercise

4. Plan and prepare (phase 1)

4.1 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); and

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

f) prioritisation or severity ratings of incidents;

g) performance measures; and

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.

4.2 Information security incident management plan

The 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; and

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.

4.3 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 responsibility and to be 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; and

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

The organisation shall conduct the following activities to ensuring the accuracy and effectiveness of the SOPs:

a) reviewed and validated;

b) distribute to all team members; and

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

4.4 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, and 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 hock 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); and

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 the incident; and

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.

4.5 Communication with external party

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

The 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.

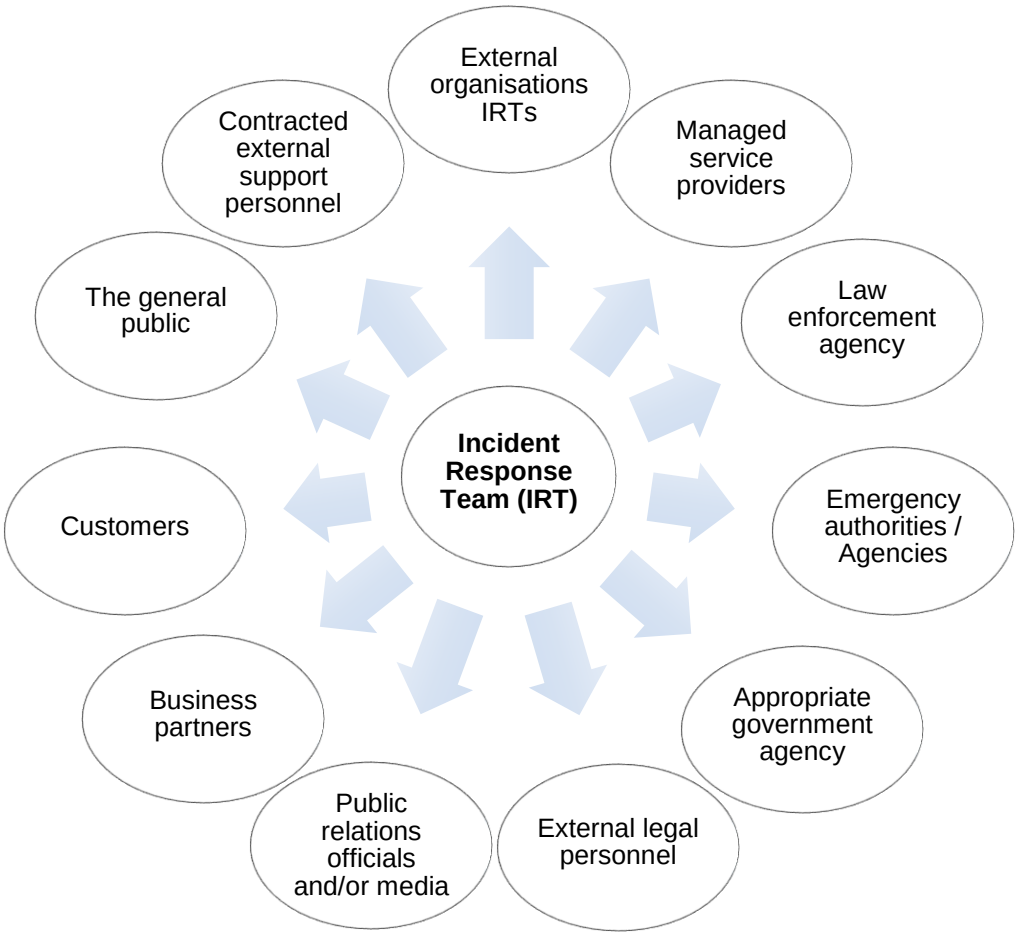

Figure 2. Relationships between the IRT and appropriate external interested parties

4.6 Awareness and training

The 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 outputs from the event/incident/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; and

h) audience and report distribution.

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

The information security incident awareness can be communicated through any means, i.e. 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.

4.7 Exercise and testing

The 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/procedures; and

c) to verify how the IRT responds to critical incidents, through the simulation of real incidents.

In the activities of the exercise and testing, the 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; and

c) ensure any changes made are subject to thorough checking, including further testing.

5. Handling an incident (phase 2)

Handling of the incident on occurrences of information security events using the information security management plan involves the process of detecting, collecting, analysing information, classifying and reporting.

5.1 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/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/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; and

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

e) facilities for information security forensics evidence collection and analysis; and

f) adequate crisis management arrangements for the information security event/incident/vulnerability database.

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

5.2 Incident detection

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

a) Activity 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;

iii) anomalies detected by audits, investigations or reviews; or

iv) suspicious events reported, to the help desk; to account managers by third parties (often customers).

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

i) report all suspected information security weakness and breaches to a central point/help desk (e.g. information failures, loss of services, detection of malicious code, denial of service attacks, errors from incomplete or inaccurate business data);

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

iii) restrain from attempting to take remedial actions themselves.

c) Activity to ensure that all involved in the POC 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); and

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

d) activity to ensure that electronic evidence is gathered and stored securely and that its secure preservation is continually monitored; and

e) activity on reporting the incident by making sure that all personnel are aware of, and have access to, information security event and incident form and details of the personnel to be notified on each occasion.

5.3 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;

b) understand the normal manners of network, system and application to enable detection of the abnormal manner;

c) establish a log retention policy, that specifies the duration of time the log data shall be maintained for future analysis;

d) correlating events among multiple indicator sources can be invaluable in validating whether a particular incident occurred;

e) networks and systems clock synchronisation;

f) deploy monitoring tools to monitor and analyse the specific traffic, performance and health; and

g) maintain and apply incident knowledge base for future reference.

5.4 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, etc.);

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; and

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

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

5.5 Incident 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.

Table 1. Severity levels based on the analyst's assessment of the impact of the attack

Severity level	Description
Informational (4)	Informational indicates routine network events with no assessed impact on the organisation. Such events are presented for informational/reporting purposes. This condition applies when there is no discernible network incident activity and no malicious code activity with a moderate or severe risk rating. Under these conditions, only a routine security posture, designed to defeat normal network threats, is warranted. Automated systems and alerting mechanisms shall be used. (Example: system scanning)
Warning (3)	The warning indicates network events that are suspicious and should require additional investigation by the organisation. They are not considered high-risk attacks and therefore do not require immediate action to mitigate the impact of the attack. This condition usually applies when knowledge or the expectation of attack activity is present, without specific events occurring or when the malicious code reaches a moderate risk rating. Under this condition, a careful examination of vulnerable and exposed systems is appropriate, security applications shall be updated with new signatures and/or rules as soon as they become available and careful monitoring of logs is recommended. Changes to the security infrastructure are not required. (Example: use of unsecure or outdated protocol (Secure Sockets Layer (SSL), Transport Layer Security (TLS) .1.0, etc.))
Critical (2)	Major functionality is severely impaired. Operations can continue in a restricted fashion, although long-term productivity might be adversely affected. A temporary workaround is available and security applications shall be updated. Critical indicates a high probability of network security incidents occurred in the organisation. Immediate action should be taken to analyse the incidents and to collaborate with other organisations if requires. (Example: virus outbreak)
Emergency (1)	Production server or other mission critical systems are not accessible and no workaround is immediately available, or on a substantial portion of the mission, critical data is at a significant risk of loss or corruption. Business operations have been severely disrupted. (Example: Distributed Denial of Service (DDoS) volumetric attack; zero days)

5.6 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)/senior management;

b) head of information security;

c) local information security officer;

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; and

k) law enforcement (if appropriate).

5.7 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:

a) blocking (and logging) of unauthorised access;

b) blocking malware sources (e.g. email addresses and websites);

c) closing particular ports and mail servers;

d) changing system administrator/super Identification (ID) passwords where compromise is suspected;

e) firewall filtering;

f) relocating website home pages;

g) isolating systems; and

h) power down affected systems.

The 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); and

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).

5.8 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; and

d) monitor the response from the attacker.

5.9 Gathering and preserving evidence

The 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 to have:

a) clear and precise evidence can be referred to for future reference including photos/image taken during incidents; and

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; and

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.

5.10 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) rebuilding infected systems (often from known 'clean' sources);

b) replacing compromised files with clean versions;

c) removing temporary constraints imposed during the containment period;

d) resetting configurations/passwords on compromised accounts (i.e. by installing patches, changing passwords and tightening network perimeter security, such as firewall rulesets);

e) testing systems thoroughly, including security controls; and

f) confirming the integrity of business systems and controls.

Upon remediation, an independent vulnerability/penetration testing of the affected systems, complemented by a security controls assessment to ensure systems are operating normally.

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

6. Post incident activities (phase 3)

6.1 Lessons learned

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 may be valuable for the following:

a) good material for training and skill gap;

b) improving incident response policies and procedures;

c) follow-up for each action item, to track the progress of every respective stakeholder to update the management 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;

f) to measure the success of the IRT; and

g) to determine if a change to incident response capabilities causes a corresponding change in the team's performance.

6.2 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; and

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. The 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 applications;

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; and

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.

6.3 Evidence retention

Organisations shall establish policy for how long evidence from an incident should be retained. The following factors shall be considered during the policy creation:

a) Prosecution

If it is possible that the attacker will be prosecuted, evidence may need to be retained until all legal actions have been completed. In some cases, this may take several years.

b) Data retention

Organisations shall have data retention policies that state how long certain types of data may be kept.

6.4 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, it's chronology, and actions are 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; and

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

6.5 Other improvements

Participation in national information security drill

Organisation categorises in the Critical National Information Infrastructure (CNII) should participate in the annual National Cyber Crisis Exercise (X-MAYA), organised by the National Security Council (NSC).

This is to ensure maximum ability on the incident response management within the organisation and ensuring that proper procedures and mechanisms are in place for effective monitoring of the CNII, incident response and reporting, communications dissemination and Business Continuity Management (BCM).

7. Information sharing (phase 4)

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

7.1 Sharing information with external party

Prior to reaching out for assistance or reporting to an external party, it is critical that the 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; and

e) the method of sharing and the protections required.

7.2 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.

Organisations trying to share information with external party shall include the following activities:

a) consult with the legal department before initiating any coordinated efforts;

b) 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); and

c) consider any existing requirements for reporting.

7.3 Information sharing methods

Information may be shared in a variety of ways depending on the objectives. The organisation shall consider the parties to share the information and the nature of the approach. Information sharing techniques may include:

a) authorised person to person;

b) electronic data transfer via the secured channel; and

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.								

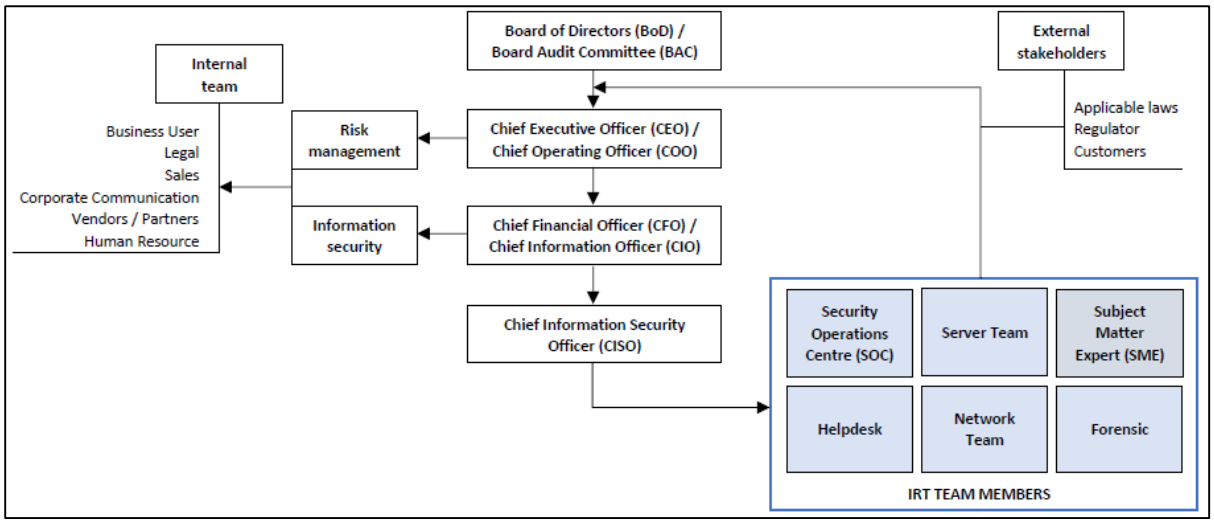

Figure A.1. Example of an information security incident structure

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 should 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, should 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 should 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

Organisations 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. Organisations 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?

Bibliography

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

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

[3] ISACA, *Incident Management and Response*

[4] MCMC Network Security Centre Standard Operating Procedure

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

Acknowledgements

Members of the Application Security Sub Working Group

Mr Azlan Mohamed Ghazali (Chairman)	Celcom Axiata Berhad
Mr Ahmad Taufik Nik Nor Azlan (Secretariat)	Malaysian Technical Standards Forum Bhd
Ms Suhana Roslan/	Al Hijrah Media Corporation
Mr Muhammad Hariz Abdul Razak	
Mr Thomas Wong	Basis Bay Malaysia
Mr Farid Mohd Thani/	Celcom Axiata Berhad
Mr Jafri Md Amin	
Ms Adzilah Abdullah/	Malaysia Digital Economy Corporation Sdn Bhd
Ms Afiqah Akmal Zainal	
Mr Muralidharan Payyapat Bhaskaran/	Maxis Communications Berhad
Mr Zulkifli M Aini	
Mr Kaw Kok Hong	MEASAT Broadcast Network Sdn Bhd
Mr Mohd Fauzi Osman/	MYTV Broadcasting Sdn Bhd
Mr Zainal Azli Rozi	
Mr Nicholas Ng/	Provintell Technologies Sdn Bhd
Mr Yew Seng Ong	
Mr Thaib Mustafa	Telekom Applied Business Sdn Bhd
Ms Nuremi Abd Halim/	Telekom Malaysia Berhad
Ms Patrina Nasiron/	
Ms Rafeah Omar	
Mr Md Azreen Shaharizan Ahmad	TIME dotCom Berhad
Prof Dr Shahrulniza/	Universiti Kuala Lumpur
Dr Megat Farez Azril Zuhairi Musa/	
Mr Mohd Taha Ismail/	
Mr Mohammad Azmin Mohamed Ghazali	
Dr Norziana Jamil	Universiti Tenaga Nasional
Mr Beng Seon Teo/	webe digital sdn bhd
Mr Chai Ko Wei	