TECHNICAL CODE

INFORMATION AND NETWORK SECURITY - CODE OF PRACTICE FOR BROADCASTING

Developed by

Malaysian Technical Standards Forum Bhd

Registered by

MCMC

Registered date:

15 October 2018

MCMC MTSFB TC G018:2018

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.mcmc.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

Committee representation

This technical code was developed by Information and Network 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

Altel Communications Sdn Bhd

MEASAT Broadcast Network Sdn Bhd (astro)

MYTV Broadcasting Sdn Bhd

Telekom Applied Business Sdn Bhd

Telekom Malaysia Berhad

Universiti Kuala Lumpur

Foreword

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

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

INFORMATION AND NETWORK SECURITY - CODE OF PRACTICE FOR BROADCASTING

0. Introduction

Digital convergence is introducing more diverse services to the world of digital broadcasting. The return channel, which enables interactive communication is key to this development and may be considered the most vulnerable element of the terminal device in terms of information security.

Accordingly, its protection from threats brought about by Internet use, such as malicious programs, is of the essence. The special characteristics of digital convergence - value networks and the secure linking of different infrastructures - need to be taken into consideration in broadcasting service development and also the service commissioning of the service.

As a service environment, digital television places very high requirements on the usability and information security solutions of services. The user group is highly heterogeneous, ranging from children to senior citizens. One cannot make many assumptions regarding the level of Information Technology (IT) know-how this group possesses. Usability of state-of-the-art terminal devices is not fully sufficient. For example, inconsistent practices in software updates of terminal devices, carried out other than within the program stream, do not increase the consumers trust in the new media.

The expectations, advantages and benefits of digital television are achieved when a consumer has the courage to, is able to and wants to use the services. The most important factor is the customer's trust in the service and its provider.

1. Scope

This Technical Code provide the guidance on the implementation of information security management for broadcasting organisations based on the requirements defined in MCMC MTSFB TC G009.

This Technical Code will allow broadcasting organisations to meet baseline information security management requirements of confidentiality, integrity, availability and any other relevant security criteria.

Broadcasting organisations refer to all individual license holders of Content Applications Service Providers (CASP), Network Facilities Provider (NFP) and Network Services Provider (NSP) for delivering end-to-end broadcasting services under the Communications and Multimedia Act 1998.

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 reference (including any amendments) applies.

See Annex A.

3. Abbreviations

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

AGM	Annual General Meeting
BCM	Business Continuity Management

BCP	Business Continuity Plan
HVAC	Heating, Ventilation and Air Conditioning
ID	Identification
IT	Information Technology
ISMS	Information Security Management Systems
ISIRT	Information Security Incident Response Team
PII	Personal Identifiable Information
PIN	Personal Identification Number
PDPA	Personal Data Protection Act
SLA	Service Level Agreement
SSO	Single Sign On
VPN	Virtual Private Network

4. Overview

4.1 Main structure

This Technical Code has been structured and closely referred to ITU-T X.1051 and ISO/IEC 27011 which contains 14 security domains.

4.1.1 Security domains

The 14 security domains include:

a) information security policies;

b) organisation of information security;

c) human resource security;

d) asset management;

e) access control;

f) cryptography;

g) physical and environmental security;

h) operations security;

i) communications security;

j) system acquisition, development and maintenance;

k) supplier relationships;

l) information security incident management;

m) information security aspects of business continuity management; and

n) compliance.

4.1.2 Control objectives

Each main security domain contains:

a) a control objective stating what is to be achieved; and

b) one or more controls that can be applied to achieve the control objective.

4.1.3 Controls

Control descriptions are structured as follows:

a) control

Defines the specific control statement, to satisfy the control objective.

b) implementation guidance

Provides more detail information to support the implementation of the control and meeting the control objective. The guidance may not be entirely suitable or sufficient in all situations and may not fulfil the broadcasting organisation's specific control requirement.

c) broadcasting-specific implementation guidance

Additional controls and implementation guidance related to broadcasting organisations are added on top of the controls above.

4.2 Information Security Management Systems (ISMS) in broadcasting

Information is an essential asset which enables broadcasting organisations to carry out their business. Information can be presented in different form such as hard copy and electronic copy, transmitted or communicated verbally, physically or electronically. Regardless of the form or the method of communication of the information, information should always be protected according to its value to the broadcasting organisations.

Information security is the preservation of:

a) Confidentiality

Property that information is not made available or disclosed to unauthorised individuals, entities, or processes.

b) Integrity

Property of accuracy and completeness.

c) Availability

Property of being accessible and usable upon demand by an authorised entity.

d) Authenticity

Property that an entity is what it is claims to be.

e) Accountability, Non-repudiation

Ability to prove the occurrence of a claimed event or action and its originating entities.

f) Reliability

Property of consistent intended behaviour and results.

Broadcasting organisations faced with numerous information risks such as physical intrusion, cyber intrusion, denial of service, human error, human fraud, natural disaster, system failure, power outage, communication infrastructure failure etc. These information risks may originate from inside or outside the broadcasting organisations. Once information security is violated, for example by unauthorised access to customer billing information, the broadcasting organisations may suffer damage financially, reputation or both. Therefore, it is essential for a broadcasting organisation to ensure its information security by implementing controls specify in this Technical Code.

4.3 Security consideration in broadcasting

It is essential that broadcasting organisations identify its information security requirement in order to meet the requirement from relevant party. Understand the needs and expectations of interested party states that organisation shall determine:

a) interested party that are relevant to the information security management system; and

b) the requirements of these interested party relevant to information security.

4.4 Information assets to be protected in broadcasting organisation

In order to secure its information, it is essential for broadcasting organisations to identify all its information assets. Example of the information assets include:

a) Information (both hardcopy and electronic copy)

Communication data, routing, subscriber, registered service, operational information, configuration, billing, business intelligent, traffic statistical analysis, contracts and agreement, system documentation, research and development, user manual, training material, standard operating procedure, network diagram, Business Continuity Plan (BCP), emergency fall back plan, audit trails, financial record, marketing and business plan, etc.

b) Information processing facilities

Any information processing system, service or infrastructure, or the physical location housing it. (Hardware, software, network facilities, network services, applications and network monitoring centre, etc.)

c) People

Broadcasting organisations' employee (customer service staff, broadcast engineers, IT, support staff, admin and finance, and staff for external party service provider or business partner, etc.)

When identifying information, it is important for broadcasting organisations to consider the information lifecycle (creation, storage, processing, use, transmission and disposal). The value of, and risks to, assets may vary during their lifecycle (unauthorised disclosure or theft of a public listed broadcasting organisation's financial report is far less significant after they have been formally published, etc).

4.5 Relevant clause specific for broadcasting

4.5.1 There are 28 clauses with specific requirement for broadcasting organisations as listed below:

a) Clause 6.1.1 Information security roles and responsibilities;

b) Clause 6.1.3 Contact with authorities;

c) Clause 6.1.4 Contact with special interest groups;

d) Clause 7.1.1 Screening;

e) Clause 7.1.2 Terms and conditions of employment;

f) Clause 8.1.1 Inventory of assets;

g) Clause 8.2.1 Classification guidelines;

h) Clause 9.1.1 Access control policy;

i) Clause 11.1.1 Physical security perimeter;

j) Clause 11.1.2 Physical entry controls;

k) Clause 11.2.1 Equipment sitting and protection;

l) Clause 11.2.2 Supporting utilities;

m) Clause 11.2.3 Cabling security;

n) Clause 12.1.1 Documented operating procedures;

o) Clause 12.1.2 Change management;

p) Clause 12.1.3 Capacity management;

q) Clause 12.1.4 Separation of development, testing and operational environments;

r) Clause 12.4.1 Event logging;

s) Clause 12.5.1 Installation of software on operational systems;

t) Clause 12.6.2 Restrictions on software installation;

u) Clause 13.1.3 Segregation in networks;

v) Clause 15.1.1 Information security policy for supplier relationships;

w) Clause 15.1.2 Addressing security within supplier agreement;

x) Clause 15.1.3 Information and communication technology supply chain;

y) Clause 16.1.6 Learning from information security incidents;

z) Clause 17.1.2 Implementing information security continuity;

aa) Clause 17.2.1 Availability of information processing facilities; and

bb) Clause 18.2.3 Technical compliance review.

5. Information security policies

5.1 Management direction for information security

To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.

5.1.1 Policies for information security

a) Control

A set of policies for information security should be defined, approved by management, published and communicated to employees and relevant external party.

b) Implementation guidance

At the highest level, organisations should define an information security policy which is approved by management and which sets out the organisation's approach to managing its information security objectives.

Information security policies should address requirements created by:

i) business strategy;

ii) regulations, legislation and contracts; and

iii) the current and projected information security threat environment.

The information security policy should contain statements concerning:

i) definition of information security, objectives and principles to guide all activities relating to information security;

ii) assignment of general and specific responsibilities for information security management to defined roles; and

iii) processes for handling deviations and exceptions.

At a lower level, the information security policy should be supported by topic specific policies, which further mandate the implementation of information security controls and are typically structured to address the needs of certain target groups within an organisation or to cover certain topics.

Examples of such policy topics include:

i) access control;

ii) information classification (and handling);

iii) physical and environmental security;

iv) end user-oriented topics such as:

1) acceptable use of assets;

2) clear desk and clear screen;

3) information transfer;

4) mobile devices and teleworking; and

5) restrictions on software installations and use.

v) backup;

vi) information transfer;

vii) protection from malware;

viii) management of technical vulnerabilities;

ix) cryptographic controls;

x) communications security;

xi) privacy and protection of personally identifiable information; and

xii) supplier relationships.

These policies should be communicated to employees and relevant external party in a form that is relevant, accessible and understandable to the intended reader, e.g. in the context of an “information security awareness, education and training programme”.

c) Other information

The need for internal policies for information security varies across organisations. Internal policies are especially useful in larger and more complex organisations where those defining and approving the expected levels of control are segregated from those implementing the controls or in situations where a policy applies to many different people or functions in the organisation. Policies for information security can be issued in a single information security policy document or as a set of individual but related documents.

If any of the information security policies are distributed outside the organisation, care should be taken not to disclose confidential information.

Some organisations use other terms for these policy documents, such as “Standards”, “Directives” or “Rules”.

5.1.2 Review of the information security policies

a) Control

The policies for information security should be reviewed at planned intervals or if significant changes occur to ensure continuing suitability, adequacy and effectiveness.

b) Implementation guidance

Each policy should have an owner who has approved management responsibility for the development, review and evaluation of the policies. The review should include assessing opportunities for improvement of the organisation’s policies and approach to managing information security in response to changes to the organisational environment, business circumstances, legal conditions or technical environment.

The review of policies for information security should take the results of management reviews into account.

Management approval for a revised policy should be obtained.

6. Organisation of information security

6.1 Internal organisation

To establish a management framework to initiate and control the implementation and operation of information security within the organisation.

6.1.1 Information security roles and responsibilities

a) Control

All information security responsibilities should be defined and allocated.

b) Implementation guidance

Allocation of information security responsibilities should be done in accordance with the information security policies. Responsibilities for the protection of individual assets and for carrying out specific information security processes should be identified. Responsibilities for information security risk management activities and in particular for acceptance of residual risks should be defined. These responsibilities should be supplemented, where necessary, with more detailed guidance for specific sites and information processing facilities. Local responsibilities for the protection of assets and for carrying out specific security processes should be defined.

Individuals with allocated information security responsibilities may delegate security tasks to others. Nevertheless, they remain accountable and should determine that any delegated tasks have been correctly performed.

Areas for which individuals are responsible should be stated. In particular the following should take place:

i) the assets and information security processes should be identified and defined;

ii) the entity responsible for each asset or information security process should be assigned and the details of this responsibility should be documented;

iii) authorisation levels should be defined and documented;

iv) to be able to fulfil responsibilities in the information security area the appointed individuals should be competent in the area and be given opportunities to keep up to date with developments: and

v) coordination and oversight of information security aspects of supplier relationships should be identified and documented.

c) Broadcasting-specific implementation guidance

Top management shall ensure that the responsibilities and authorities for roles relevant to information security are assigned and communicated. Security roles and responsibilities shall be defined and clearly communicated during the employment process and documented in relevant employment document.

d) Other information

Many organisations appoint an information security manager to take overall responsibility for the development and implementation of information security and to support the Identification (ID) of controls.

However, responsibility for resourcing and implementing the controls will often remain with individual managers. One common practice is to appoint an owner for each asset who then becomes responsible for its day to day protection.

6.1.2 Segregation of duties

a) Control

Conflicting duties and areas of responsibility should be segregated to reduce opportunities for unauthorised or unintentional modification or misuse of the organisation's assets.

b) Implementation guidance

Care should be taken that no single person can access, modify or use assets without authorisation or detection. The initiation of an event should be separated from its authorisation. The possibility of collusion should be considered in designing the controls.

Small organisations may find segregation of duties difficult to achieve, but the principle should be applied as far as is possible and practicable. Whenever it is difficult to segregate, other controls such as monitoring of activities, audit trails and management supervision should be considered.

c) Other Information

Broadcasting organisations should ensure that no single person can access, modify or use assets without authorisation or detection, e.g. separation of operating system and database administration. It may not be able to apply in all circumstances but it should be applied as far as possible and practicable.

6.1.3 Contact with authorities

a) Control

Appropriate contacts with relevant authorities should be maintained.

b) Implementation guidance

Organisations should have procedures in place that specify when and by whom authorities (e.g. law enforcement, regulatory bodies, supervisory authorities) should be contacted and how identified information security incidents should be reported in a timely manner (e.g. if it is suspected that laws may have been broken).

c) Broadcasting-specific implementation guidance

Broadcasting organisations should have procedures in place that specify when and by whom authorities (e.g. law enforcement, regulatory bodies, supervisory authorities) should be contacted and how identified information security incidents should be reported in a timely manner (e.g. if it is suspected that laws may be been broken). Maintaining such contacts may be a requirement to support information security incident management. Contacts with regulatory bodies are also useful to anticipate and prepare for upcoming changes in law or regulations, which have to be implemented by the broadcasting organisations.

Contacts with other authorities include utilities, emergency services, electricity supplier, health and safety which may affect the operating environment (e.g. crime rate, utility outage, natural disaster - flood, fire, and earthquake) are equally important in order to avoid any interruption to the broadcasting services.

d) Other information

Organisations under attack from the Internet may need authorities to take action against the attack source.

Maintaining such contacts may be a requirement to support information security incident management or the business continuity and contingency planning process. Contacts with regulatory bodies are also useful to anticipate and prepare for upcoming changes in laws or regulations, which have to be implemented by the organisation. Contacts with other authorities include utilities, emergency services, electricity suppliers and health and safety, e.g. fire departments (in connection with business continuity), broadcasting providers (in connection with line routing and availability) and water suppliers (in connection with cooling facilities for equipment).

Table 1 shows some examples of authorities and their subject matter:

Table 1. Example of authorities and their subject matter

Authorities/Utilities	Subject Matter
Polis Diraja Malaysia	Crime rate in respective area that may affect the broadcasting facilities.
Jabatan Bomba dan Penyelamat Malaysia	Fire hazard especially forest fire that may affect the broadcasting facilities
Jabatan Pengairan dan Saliran Malaysia (http://www.water.gov.my)	Information related to flood that may affect broadcasting facilities
Jabatan Meteorologi Malaysia (http://www.met.gov.my)	Information related to weather, wind, storm, earthquake and etc that may affect broadcasting facilities
Dewan Bandaraya, Majlis Perbandaran, Majlis Daerah, Pihak Berkuasa Tempatan	Information related to rules and regulation that may affect the construction, maintenance, renovation, expansion of the broadcasting facilities.
Tenaga Nasional Bhd, Sabah Electricity Sdn Bhd, Sarawak Energy Bhd	Information related to electricity supply to the broadcasting facilities.
Suruhanjaya Komunikasi dan Multimedia Malaysia (MCMC)	Information on regulations for communications and multimedia industry

6.1.4 Contact with special interest groups

a) Control

Appropriate contacts with special interest groups or other specialist security forums and professional associations should be maintained.

b) Broadcast-specific implementation guidance

Participation on special interest group may include but not limited to forum, workgroup, workshop, newsgroup, newsletter etc. The objectives of the participation in special interest group are:

i) improve knowledge about best practices, weaknesses and stay up to date on the information processing facilities used by broadcasting organisations;

ii) ensure the understanding of information security environment is current and complete;

iii) receive early warning of alerts, advisories and patches pertaining to attacks and vulnerabilities; and

iv) gain access to specialist information security advice.

c) Other information

Information sharing agreement can be establish to improve cooperation and coordination of security issue.

Example of useful internet site related to information security in broadcasting industry:

i) mcmc.gov.my;

ii) sebenarnya.my;

iii) www.cmcf.my;

iv) www.mycert.org.my; and

v) www.cfm.my.

6.1.5 Information security in project management

a) Control

Information security should be addressed in project management, regardless of the type of the project.

b) Implementation guidance

Information security should be integrated into the organisation's project management methodology to ensure that information security risk is identified and addressed as part of a project. This applies generally to any project regardless of its character, e.g. a project for a core business process, IT, transmission infrastructure, facility management, content and other supporting processes. The project management methodology in use should require that:

i) information security objectives are included in project objectives, and all the phases of the applied project methodology;

ii) identify the risk owner, e.g. project manager and define the roles and responsibilities;

iii) conduct information security risk assessment at the early stage of the project and identify necessary control to mitigate the risk to an acceptable level; and

iv) review the risk and the effectiveness of control implemented periodically or in the event of any significant changes that may affect the information security.

6.2 Mobile devices and teleworking

To ensure the security of teleworking and use of mobile devices.

6.2.1 Mobile device policy

a) Control

A policy and supporting security measures should be adopted to manage the risks introduced by using mobile devices.

b) Implementation guidance

When using mobile devices, special care should be taken to ensure that business information is not compromised. The mobile device policy should take into account the risks of working with mobile devices in unprotected environments.

The mobile device policy should consider:

i) Registration of mobile devices;

ii) requirements for physical protection;

iii) restriction of software installation;

iv) requirements for mobile device software versions and for applying patches;

v) restriction of connection to information services;

vi) access controls;

vii) cryptographic techniques;

viii) malware protection;

ix) remote disabling, erasure or lockout;

x) backups; and

xi) usage of web services and web apps.

Care should be taken when using mobile devices in public places, meeting rooms and other unprotected areas. Protection should be in place to avoid the unauthorised access to or disclosure of the information stored and processed by these devices, e.g. using cryptographic techniques and enforcing use of secret authentication information.

Mobile devices should also be physically protected against theft especially when left, for example, in cars and other forms of transport, hotel rooms, conference centres and meeting places. A specific procedure taking into account legal, insurance and other security requirements of the organisation should be established for cases of theft or loss of mobile devices. Devices carrying important, sensitive or critical business information should not be left unattended and, where possible, should be physically locked away, or special locks should be used to secure the devices.

Training should be arranged for personnel using mobile devices to raise their awareness of the additional risks resulting from this way of working and the controls that should be implemented. Where the mobile device policy allows the use of privately owned mobile devices, the policy and related security measures should also consider:

i) separation of private and business use of the devices, including using software to support such separation and protect business data on a private device; and

ii) providing access to business information only after users have signed an end user agreement acknowledging their duties (physical protection, software updating, etc.), waiving ownership of business data, allowing remote wiping of data by the organisation in case of theft or loss of the device or when no longer authorised to use the service. This policy needs to take account of privacy legislation.

c) Other information

Mobile device wireless connections are similar to other types of network connection but have important differences that should be considered when identifying controls. Typical differences are:

i) some wireless security protocols are immature and have known weaknesses; and

ii) information stored on mobile devices may not be backed-up because of limited network bandwidth or because mobile devices may not be connected at the times when backups are scheduled.

Mobile devices generally share common functions, e.g. networking, internet access, e-mail and file handling, with fixed use devices. Information security controls for the mobile devices generally consist of those adopted in the fixed use devices and those to address threats raised by their usage outside the organisation's premises.

6.2.2 Teleworking

a) Control

A policy and supporting security measures should be implemented to protect information accessed, processed or stored at teleworking sites.

b) Implementation guidance

Organisations allowing teleworking activities should issue a policy that defines the conditions and restrictions for using teleworking. Where deemed applicable and allowed by law, the following matters should be considered:

i) the existing physical security of the teleworking site, taking into account the physical security of the building and the local environment;

ii) the proposed physical teleworking environment;

iii) the communications security requirements, taking into account the need for remote access to the organisation's internal systems, the sensitivity of the information that will be accessed and passed over the communication link and the sensitivity of the internal system;

iv) the provision of virtual desktop access that prevents processing and storage of information on privately owned equipment;

v) the threat of unauthorised access to information or resources from other persons using the accommodation, e.g. family and friends;

vi) the use of home networks and requirements or restrictions on the configuration of wireless network services;

vii) policies and procedures to prevent disputes concerning rights to intellectual property developed on privately owned equipment;

viii) access to privately owned equipment (to verify the security of the machine or during an investigation), which may be prevented by legislation;

ix) software licensing agreements that are such that organisations may become liable for licensing for client software on workstations owned privately by employees or external party users; and

x) malware protection and firewall requirements.

The guidelines and arrangements to be considered should include:

i) the provision of suitable equipment and storage furniture for the teleworking activities, where the use of privately owned equipment that is not under the control of the organisation is not allowed;

ii) a definition of the work permitted, the hours of work, the classification of information that may be held and the internal systems and services that the teleworker is authorised to access;

iii) the provision of suitable communication equipment, including methods for securing remote access;

iv) physical security;

v) rules and guidance on family and visitor access to equipment and information;

vi) the provision of hardware and software support and maintenance;

vii) the provision of insurance;

viii) the procedures for backup and business continuity;

ix) audit and security monitoring; and

x) revocation of authority and access rights, and the return of equipment when the teleworking activities are terminated.

c) Other information

Teleworking refers to all forms of work outside of the office, including non-traditional work environments, such as those referred to as “telecommuting”, “flexible workplace”, “remote work” and “virtual work” environments.

7. Human resource security

7.1 Prior to employment

To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered.

7.1.1 Screening

a) Control

Background verification checks on all candidates for employment (directly or indirectly) should be carried out in accordance with relevant laws, regulations and ethics and should be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.

b) Implementation guidance

Verification should take into account all relevant privacy, protection of personally identifiable information and employment-based legislation, and should, where permitted, include the following:

i) availability of satisfactory character references, e.g. one business and one personal;

ii) a verification (for completeness and accuracy) of the applicant's curriculum vitae;

iii) confirmation of claimed academic and professional qualifications;

iv) independent identity verification (passport or similar document); and

v) more detailed verification, such as credit review or review of criminal records.

When an individual is hired for a specific information security role, organisations should make sure the candidate:

i) has the necessary competence to perform the security role; and

ii) can be trusted to take on the role, especially if the role is critical for the organisation.

Where a job, either on initial appointment or on promotion, involves the person having access to information processing facilities, and, in particular, if these are handling confidential information, e.g. financial information or highly confidential information, the organisation should also consider further, more detailed verifications.

Procedures should define criteria and limitations for verification reviews, e.g. who is eligible to screen people and how, when and why verification reviews are carried out.

A screening process should also be ensured for contractors. In these cases, the agreement between the organisation and the contractor should specify responsibilities for conducting the screening and the notification procedures that need to be followed if screening has not been completed or if the results give cause for doubt or concern.

Information on all candidates being considered for positions within the organisation should be collected and handled in accordance with any appropriate legislation existing in the relevant jurisdiction. Depending on applicable legislation, the candidates should be informed beforehand about the screening activities.

c) Broadcasting-specific implementation guidance

Procedures should be established to define the criteria and the roles and responsibilities to carry out the screening process. Verification should take into account all relevant privacy, protection of Personal Identifiable Information (PII) and employment based legislation, and should, where permitted.

The screening process should also be ensured for contractors, business partners or any other relevant party who may access broadcasting organisations' information and/or information processing facilities. In these cases, the agreement between the broadcasting organisations the relevant party should specify responsibilities for conducting the screening and the notifications procedures that need to be followed if screening has not been completed or if the results give cause for doubt or concern.

7.1.2 Terms and conditions of employment

a) Control

The contractual agreements with employees and contractors should state theirs and the organisation's responsibilities for information security.

b) Implementation guidance

The contractual obligations for employees or contractors should reflect the organisation's policies for information security in addition to clarifying and stating:

i) That all employees and contractors who are given access to confidential information should sign a confidentiality or non-disclosure agreement prior to being given access to information processing facilities.

ii) The employee's or contractor's legal responsibilities and rights, e.g. regarding copyright laws or data protection legislation.

iii) Responsibilities for the classification of information and management of organisational assets associated with information, information processing facilities and information services handled by the employee or contractor.

iv) Responsibilities of the employee or contractor for the handling of information received from other companies or external party.

v) Actions to be taken if the employee or contractor disregards the organisation's security requirements.

Information security roles and responsibilities should be communicated to job candidates during the pre-employment process.

The organisation should ensure that employees and contractors agree to terms and conditions concerning information security appropriate to the nature and extent of access they will have to the organisation's assets associated with information systems and services.

Where appropriate, responsibilities contained within the terms and conditions of employment should continue for a defined period after the end of the employment.

c) Broadcasting-specific implementation guidance

The legal rights and responsibilities regarding non-disclosure of communications and essential communications, which broadcasting organisations should take into account, are included in the laws and regulations.

Broadcasting organisations should clarify and state the responsibilities for maintaining the communications service provided by broadcasting organisations in addition to the protection and non-disclosure of personally identifiable and other confidential information in the terms and conditions of employment.

Broadcasting organisations should make sure that any person engaged in their broadcasting services is aware and up to date on:

i) their responsibilities for protecting the PII on and other confidential information of users of their service; and

ii) their responsibilities concerning the non-disclosure of privileged information obtained through their operational activities on broadcasting services.

d) Other information

A code of conduct may be used to state the employee's or contractor's information security responsibilities regarding confidentiality, data protection, ethics, appropriate use of the organisation's equipment and facilities, as well as reputable practices expected by the organisation.

An external party, with which a contractor is associated, can be required to enter into contractual arrangements on behalf of the contracted individual.

7.2 During employment

To ensure that employees and contractors are aware of and fulfil their information security responsibilities.

7.2.1 Management responsibilities

a) Control

Management should require all employees and contractors to apply information security in accordance with the established policies and procedures of the organisation.

b) Implementation guidance

Management responsibilities should include ensuring that employees and contractors:

i) are properly briefed on their information security roles and responsibilities prior to being granted access to confidential information or information systems;

ii) are provided with guidelines to state information security expectations of their role within the organisation;

iii) are motivated to fulfil the information security policies of the organisation;

iv) achieve a level of awareness on information security relevant to their roles and responsibilities within the organisation;

v) conform to the terms and conditions of employment, which includes the organisation's information security policy and appropriate methods of working;

vi) continue to have the appropriate skills and qualifications and are educated on a regular basis; and

vii) are provided with an anonymous reporting channel to report violations of information security policies or procedures ("whistle blowing").

Management should demonstrate support of information security policies, procedures and controls, and act as a role model.

c) Other information

If employees and contractors are not made aware of their information security responsibilities, they can cause considerable damage to an organisation. Motivated personnel are likely to be more reliable and cause fewer information security incidents.

Poor management can cause personnel to feel undervalued resulting in a negative information security impact on the organisation. For example, poor management can lead to information security being neglected or potential misuse of the organisation's assets.

7.2.2 Information security awareness, education and training

a) Control

All employees of the organisation and, where relevant, contractors should receive appropriate awareness education and training and regular updates in organisational policies and procedures, as relevant for their job function.

b) Implementation guidance

An information security awareness programme should aim to make employees and, where relevant, contractors aware of their responsibilities for information security and the means by which those responsibilities are discharged.

An information security awareness programme should be established in line with the organisation's information security policies and relevant procedures, taking into consideration the organisation's information to be protected and the controls that have been implemented to protect the information.

The awareness programme should include a number of awareness-raising activities such as campaigns (e.g. an "information security day") and issuing booklets or newsletters. The awareness programme should be planned taking into consideration the employees' roles in the organisation, and, where relevant, the organisation's expectation of the awareness of contractors. The activities in the awareness programme should be scheduled over time, preferably regularly, so that the activities are repeated and cover new employees and contractors. The awareness programme should also be updated regularly, in line with organisational policies and procedures, and should be built on lessons learnt from information security incidents.

Awareness training should be performed as required by the organisation's information security awareness programme. Awareness training can use different delivery media including classroom-based, distance learning, web-based, self-paced and others.

Information security education and training should also cover general aspects which includes:

i) stating management's commitment to information security throughout the organisation;

ii) the need to become familiar with and comply with applicable information security rules and obligations, as defined in policies, standards, laws, regulations, contracts and agreements;

iii) personal accountability for one's own actions and inactions, and general responsibilities towards securing or protecting information belonging to the organisation and external party;

iv) basic information security procedures (e.g. information security incident reporting) and baseline controls (such as password security, malware controls and clear desks); and

v) contact points and resources for additional information and advice on information security matters, including further information security education and training materials.

Information security education and training should take place periodically. Initial education and training applies to those who transfer to new positions or roles with substantially different information security requirements, not limited to new starters and should take place before the role becomes active.

The organisation should develop the education and training programme in order to conduct the education and training effectively. The programme should be in line with the organisation's information security policies and relevant procedures, taking into consideration the organisation's information to be protected and the controls that have been implemented to protect the information. The programme should consider different forms of education and training, e.g. lectures or self-studies.

c) Other information

When composing an awareness programme, it is important not only to focus on the 'what' and 'how', but also the 'why'. It is important that employees understand the aim of information security and the potential impact, positive and negative, on the organisation of their own behaviour.

Awareness, education and training can be part of, or conducted in collaboration with, other training activities, for example general IT or general security training. Awareness, education and training activities should be suitable and relevant to the individual's roles, responsibilities and skills.

An assessment of the employees' understanding could be conducted at the end of an awareness, education and training course to test knowledge transfer.

7.2.3 Disciplinary process

a) Control

There should be a formal and communicated disciplinary process in place to take action against employees who have committed an information security breach.

b) Implementation guidance

The disciplinary process should not be commenced without prior verification that an information security breach has occurred.

The formal disciplinary process should ensure correct and fair treatment for employees who are suspected of committing breaches of information security. The formal disciplinary process should provide for a graduated response that takes into consideration factors such as the nature and gravity of the breach and its impact on business, whether or not this is a first or repeat offence, whether or not the violator was properly trained, relevant legislation, business contracts and other factors as required.

The disciplinary process should also be used as a deterrent to prevent employees from violating the organisation's information security policies and procedures and any other information security breaches. Deliberate breaches may require immediate actions.

c) Other information

The disciplinary process can also become a motivation or an incentive if positive sanctions are defined for remarkable behaviour with regards to information security.

7.3 Termination or change of employment

To protect the organisation's interests as part of the process of changing or terminating employment.

7.3.1 Termination or change of employment responsibilities

a) Control

Information security responsibilities and duties that remain valid after termination or change of employment should be defined, communicated to the employee or contractor and enforced.

b) Implementation guidance

The communication of termination responsibilities should include on-going information security requirements and legal responsibilities and, where appropriate, responsibilities contained within any confidentiality agreement and the terms and conditions of employment continuing for a defined period after the end of the employee's or contractor's employment.

Responsibilities and duties still valid after termination of employment should be contained in the employee's or contractor's terms and conditions of employment.

Changes of responsibility or employment should be managed as the termination of the current responsibility or employment combined with the initiation of the new responsibility or employment.

c) Other information

The human resources function is generally responsible for the overall termination process and works together with the supervising manager of the person leaving to manage the information security aspects of the relevant procedures. In the case of a contractor provided through an external party, this termination process is undertaken by the external party in accordance with the contract between the organisation and the external party.

It may be necessary to inform employees, customers or contractors of changes to personnel and operating arrangements.

8. Asset management

8.1 Responsibility for assets

To identify organisational assets and define appropriate protection responsibilities.

8.1.1 Inventory of assets

a) Control

Assets associated with information and information processing facilities should be identified and an inventory of these assets should be drawn up and maintained.

b) Implementation guidance

An organisation should identify assets relevant in the lifecycle of information and document their importance. The lifecycle of information should include creation, processing, storage, transmission, deletion and destruction. Documentation should be maintained in dedicated or existing inventories as appropriate.

The asset inventory should be accurate, up to date, aligned and consistent with other inventories.

For each of the identified assets, ownership of the asset should be assigned and the classification should be identified.

c) Broadcasting-specific implementation guidance

When developing and maintaining the inventory of assets, clear responsibilities between the broadcasting facilities of the organisation and those of other connected or related broadcasting organisations should be specified and clearly documented.

Inventories of assets help to ensure that effective asset protection take place, and may also be required for other business purposes, such as health and safety, maintenance, capacity planning, business continuity, insurance or finance (asset management) reasons.

8.1.2 Ownership of assets

a) Control

Assets maintained in the inventory should be owned.

b) Implementation guidance

Individuals as well as other entities having approved management responsibility for the asset lifecycle qualify to be assigned as asset owners.
A process to ensure timely assignment of asset ownership is usually implemented. Ownership should be assigned when assets are created or when assets are transferred to the organisation. The asset owner should be responsible for the proper management of an asset over the whole asset lifecycle.

The asset owner should:

i) ensure that assets are inventoried;

ii) ensure that assets are appropriately classified and protected;

iii) define and periodically review access restrictions and classifications to important assets, taking into account applicable access control policies; and

iv) ensure proper handling when the asset is deleted or destroyed.

c) Other information

The identified owner can be either an individual or an entity who has approved management responsibility for controlling the whole lifecycle of an asset. The identified owner does not necessarily have any property rights to the asset.

Routine tasks may be delegated, e.g. to a custodian looking after the assets on a daily basis, but the responsibility remains with the owner.

In complex information systems, it may be useful to designate groups of assets which act together to provide a particular service. In this case the owner of this service is accountable for the delivery of the service, including the operation of its assets.

8.1.3 Acceptable use of assets

a) Control

Rules for the acceptable use of information and of assets associated with information and information processing facilities should be identified, documented and implemented.

b) Implementation guidance

Employees and external party users using or having access to the organisation's assets should be made aware of the information security requirements of the organisation's assets associated with information and information processing facilities and resources. They should be responsible for their use of any information processing resources and of any such use carried out under their responsibility.

8.1.4 Return of assets

a) Control

All employees and external party users should return all of the organisational assets in their possession upon termination of their employment, contract or agreement.

b) Implementation guidance

The termination process should be formalised to include the return of all previously issued physical and electronic assets owned by or entrusted to the organisation.

In cases where an employee or external party user purchases the organisation's equipment or uses their own personal equipment, procedures should be followed to ensure that all relevant information is transferred to the organisation and securely erased from the equipment.
In cases where an employee or external party user has knowledge that is important to ongoing operations, that information should be documented and transferred to the organisation.

During the notice period of termination, the organisation should control unauthorised copying of relevant information (e.g. intellectual property) by terminated employees and contractors.

8.2 Information classification

To ensure that information receives an appropriate level of protection in accordance with its importance to the organisation.

8.2.1 Classification guidelines

a) Control

Information should be classified in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification.

b) Implementation guidance

Classifications and associated protective controls for information should take account of business needs for sharing or restricting information, as well as legal requirements. Assets other than information can also be classified in conformance with classification of information which is stored in, processed by or otherwise handled or protected by the asset.

Owners of information assets should be accountable for their classification.

The classification scheme should include conventions for classification and criteria for review of the classification over time. The level of protection in the scheme should be assessed by analysing confidentiality, integrity and availability and any other requirements for the information considered. The scheme should be aligned to the access control policy.

Each level should be given a name that makes sense in the context of the classification scheme's application.

The scheme should be consistent across the whole organisation so that everyone will classify information and related assets in the same way, have a common understanding of protection requirements and apply the appropriate protection.

Classification should be included in the organisation's processes and be consistent and coherent across the organisation. Results of classification should indicate value of assets depending on their sensitivity and criticality to the organisation, e.g. in terms of confidentiality, integrity and availability.

Results of classification should be updated in accordance with changes of their value, sensitivity and criticality through their life cycle.

c) Broadcasting-specific implementation guidance

Classifications and associated protective controls for information should take account of business needs for sharing or restricting information, as well as legal requirements (e.g. Personal Data Protection Act (PDPA) 2010, Contractual agreement). Information processing facilities also can be classified in conformance with classification of information which is stored in, processed by or otherwise handle by the facilities.

The classification scheme should be consistent across the entire broadcasting organisations so that everyone will classify information and related information processing facilities in the same way, have a common understanding of protection requirements and apply appropriate control.

d) Other information

Classification provides people who deal with information with a concise indication of how to handle and protect it. Creating groups of information with similar protection needs and specifying information security procedures that apply to all the information in each group facilitates this. This approach reduces the need for case by case risk assessment and custom design of controls.
Information can conclude to be sensitive or critical after a certain period of time, for example, when the information has been made public. These aspects should be taken into account, as over classification can lead to the implementation of unnecessary controls resulting in additional expense or on the contrary under-classification can endanger the achievement of business objectives.

An example of an information confidentiality classification scheme could be based on four levels as follows:

i) disclosure causes no harm;

ii) disclosure causes minor embarrassment or minor operational inconvenience;

iii) disclosure has a significant short-term impact on operations or tactical objectives; and

iv) disclosure has a serious impact on long term strategic objectives or puts the survival of the organisation at risk.

8.2.2 Labelling of information

a) Control

An appropriate set of procedures for information labelling should be developed and implemented in accordance with the information classification scheme adopted by the organisation.

b) Implementation guidance

Procedures for information labelling need to cover information and its related assets in physical and electronic formats. The labelling should reflect the classification scheme established. The labels should be easily recognisable. The procedures should give guidance on where and how labels are attached in consideration of how the information is accessed or the assets are handled depending on the types of media. The procedures can define cases where labelling is omitted, e.g. labelling of non-confidential information to reduce workloads. Employees and contractors should be made aware of labelling procedures.

Output from systems containing information that is classified as being sensitive or critical should carry an appropriate classification label.

c) Other information

Labelling of classified information is a key requirement for information sharing arrangements. Physical labels and metadata are a common form of labelling.

Labelling of information and its related assets can sometimes have negative effects. Classified assets are easier to identify and accordingly to steal by insiders or external attackers.

8.2.3 Handling of assets

a) Control

Procedures for handling assets should be developed and implemented in accordance with the information classification scheme adopted by the organisation.

b) Implementation guidance

Procedures should be drawn up for handling, processing, storing and communicating information consistent with its classification.

The following items should be considered:

i) access restrictions supporting the protection requirements for each level of classification;

ii) maintenance of a formal record of the authorised recipients of assets;

iii) protection of temporary or permanent copies of information to a level consistent with the protection of the original information;

iv) storage of IT assets in accordance with manufacturers' specifications; and

v) clear marking of all copies of media for the attention of the authorised recipient.

The classification scheme used within the organisation may not be equivalent to the schemes used by other organisations, even if the names for levels are similar; in addition, information moving between organisations can vary in classification depending on its context in each organisation, even if their classification schemes are identical.

Agreements with other organisations that include information sharing should include procedures to identify the classification of that information and to interpret the classification labels from other organisation.

8.3 Media handling

To prevent unauthorised disclosure, modification, removal or destruction of information stored on media.

8.3.1 Management of removable media

a) Control

Procedures should be implemented for the management of removable media in accordance with the classification scheme adopted by the organisation.

b) Implementation guidance

The following guidelines for the management of removable media should be considered:

i) if no longer required, the contents of any reusable media that are to be removed from the organisation should be made unrecoverable;

ii) where necessary and practical, authorisation should be required for media removed from the organisation and a record of such removals should be kept in order to maintain an audit trail;

iii) all media should be stored in a safe, secure environment, in accordance with manufacturers' specifications;

iv) if data confidentiality or integrity are important considerations, cryptographic techniques should be used to protect data on removable media;

v) to mitigate the risk of media degrading while stored data are still needed, the data should be transferred to fresh media before becoming unreadable;

vi) multiple copies of valuable data should be stored on separate media to further reduce the risk of coincidental data damage or loss;

vii) registration of removable media should be considered to limit the opportunity for data loss;

viii) removable media drives should only be enabled if there is a business reason for doing so; and

ix) where there is a need to use removable media the transfer of information to such media should be monitored.

Procedures and authorisation levels should be documented.

8.3.2 Disposal of media

a) Control

Media should be disposed of securely when no longer required, using formal procedures.

b) Implementation guidance

Formal procedures for the secure disposal of media should be established to minimise the risk of confidential information leakage to unauthorised persons. The procedures for secure disposal of media containing confidential information should be proportional to the sensitivity of that information. The following items should be considered:

i) media containing confidential information should be stored and disposed of securely, e.g. by incineration or shredding, or erasure of data for use by another application within the organisation;

ii) procedures should be in place to identify the items that might require secure disposal;

iii) it may be easier to arrange for all media items to be collected and disposed of securely, rather than attempting to separate out the sensitive items;

iv) many organisations offer collection and disposal services for media; care should be taken in selecting a suitable external party with adequate controls and experience; and

v) disposal of sensitive items should be logged in order to maintain an audit trail.

When accumulating media for disposal, consideration should be given to the aggregation effect, which can cause a large quantity of non-sensitive information to become sensitive.

c) Other information

Damaged devices containing sensitive data may require a risk assessment to determine whether the items should be physically destroyed rather than sent for repair or discarded.

8.3.3 Physical media transfer

a) Control

Media containing information should be protected against unauthorised access, misuse or corruption during transportation.

b) Implementation guidance

The following guidelines should be considered to protect media containing information being transported:

i) reliable transport or couriers should be used;

ii) a list of authorised couriers should be agreed with management;

iii) procedures to verify the ID of couriers should be developed;

iv) packaging should be sufficient to protect the contents from any physical damage likely to arise during transit and in accordance with any manufacturers' specifications, for example protecting against any environmental factors that may reduce the media's restoration effectiveness such as exposure to heat, moisture or electromagnetic fields; and

v) logs should be kept, identifying the content of the media, the protection applied as well as recording the times of transfer to the transit custodians and receipt at the destination.

c) Other information

Information can be vulnerable to unauthorised access, misuse or corruption during physical transport, for instance when sending media via the postal service or via courier. In this control, media include paper documents.

When confidential information on media is not encrypted, additional physical protection of the media should be considered.

9. Access control

9.1 Business requirement for access control

To limit access to information and information processing facilities.

9.1.1 Access control policy

a) Control

An access control policy should be established, documented and reviewed based on business and information security requirements.

b) Implementation guidance

Asset owners should determine appropriate access control rules, access rights and restrictions for specific user roles towards their assets, with the amount of detail and the strictness of the controls reflecting the associated information security risks.

Access controls are both logical and physical and these should be considered together. Users and service providers should be given a clear statement of the business requirements to be met by access controls.

The policy should take account of the following:

i) security requirements of business applications;

ii) policies for information dissemination and authorisation, e.g. the need-to-know principle and information security levels and classification of information;

iii) consistency between the access rights and information classification policies of systems and networks;

iv) relevant legislation and any contractual obligations regarding limitation of access to data or services;

v) management of access rights in a distributed and networked environment which recognises all types of connections available;

vi) segregation of access control roles, e.g. access request, access authorisation, access administration;

vii) requirements for formal authorisation of access requests;

viii) requirements for periodic review of access rights;

ix) removal of access rights;

x) archiving of records of all significant events concerning the use and management of user identities and secret authentication information; and

xi) roles with privileged access.

c) Broadcasting-specific implementation guidance

Broadcasting organisations should implement role-based access controls, with a limited number of profiles and controlled sets of user access permissions as applicable.

As broadcasting companies are regularly exposed to different suppliers that may not support the same security features or standards, it is essential to ensure all access is tracked for amendments and timely removal.

Only the authorised users should have access to use the broadcasting services.

d) Other information

Care should be taken when specifying access control rules to consider:

i) establishing rules based on the premise “Everything is generally forbidden unless expressly permitted” rather than the weaker rule “Everything is generally permitted unless expressly forbidden”;
ii) changes in information labels that are initiated automatically by information processing facilities and those initiated at the discretion of a user;

iii) changes in user permissions that are initiated automatically by the information system and those initiated by an administrator; and

iv) rules which require specific approval before enactment and those which do not.

Access control rules should be supported by formal procedures and defined responsibilities.

Role based access control is an approach used successfully by many organisations to link access rights with business roles.

Two of the frequent principles directing the access control policy are:

i) Need-to-know: you are only granted access to the information you need to perform your tasks (different tasks/roles mean different need-to-know and hence different access profile); and

ii) Need-to-use: you are only granted access to the information processing facilities (IT equipment, applications, procedures, rooms) you need to perform your task/job/role.

9.1.2 Access to networks and network services

a) Control

Users should only be provided with access to the network and network services that they have been specifically authorised to use.

b) Implementation guidance

A policy should be formulated concerning the use of networks and network services. This policy should cover:

i) the networks and network services which are allowed to be accessed;

ii) authorisation procedures for determining who is allowed to access which networks and networked services;

iii) management controls and procedures to protect access to network connections and network services;

iv) the means used to access networks and network services (e.g. use of Virtual Private Network (VPN) or wireless network);

v) user authentication requirements for accessing various network services; and

vi) monitoring of the use of network services.

The policy on the use of network services should be consistent with the organisation's access control policy.

c) Broadcasting-specific implementation guidance (transmission)

Unauthorised and insecure connections to network services can affect the whole organisation. This control is particularly important for network connections to sensitive or critical business applications (e.g. Command centre) or to users in high risk location, e.g. public or external areas that are outside the organisation's information security management and control.
A policy aligns with broadcasting organisation's access control policy) should be formulated concerning the use of networks and network services. This policy should cover:

i) the networks and network services (broadcasting network, equipment management network, corporate network, financial network) which are allowed to be accessed;

ii) segregation of access control roles, e.g. access request, access authorisation, access administration;

iii) the means used to access network and network services (e.g. use of VPN or wireless network) securely;

iv) extra care should be given to the access to broadcasting network and monitoring segment, avoid wireless network due to lower security control and connection reliability; and

v) the use of the network services should be monitored constantly to detect any non-compliance with the access control policy (should the network services provided by third party, broadcasting organisations should monitor the services regularly).

9.2 User access management

To ensure authorised user access and to prevent unauthorised access to systems and services.

9.2.1 User registration and de-registration

a) Control

A formal user registration and de-registration process should be implemented to enable assignment of access rights.

b) Implementation guidance

The process for managing user ID should include:

i) using unique user IDs to enable users to be linked to and held responsible for their actions; the use of shared IDs should only be permitted where they are necessary for business or operational reasons and should be approved and documented;

ii) immediately disabling or removing user IDs of users who have left the organisation;

iii) periodically identifying and removing or disabling redundant user IDs; and

iv) ensuring that redundant user IDs are not issued to other users.

c) Other information

Providing or revoking access to information or information processing facilities is usually a two (2) step procedure:

i) assigning and enabling, or revoking, a user ID; and

ii) providing, or revoking, access rights to such user ID.

9.2.2 User access provisioning

a) Control

A formal user access provisioning process should be implemented to assign or revoke access rights for all user types to all systems and services.

b) Implementation guidance

The provisioning process for assigning or revoking access rights granted to user IDs should include:

i) obtaining authorisation from the owner of the information system or service for the use of the information system or service; separate approval for access rights from management may also be appropriate;

ii) verifying that the level of access granted is appropriate to the access policies and is consistent with other requirements such as segregation of duties;

iii) ensuring that access rights are not activated (e.g. by service providers) before authorisation procedures are completed;

iv) maintaining a central record of access rights granted to a user ID to access information systems and services;

v) adapting access rights of users who have changed roles or jobs and immediately removing or blocking access rights of users who have left the organisation; and

vi) periodically reviewing access rights with owners of the information systems or services.

c) Other information

Consideration should be given to establishing user access roles based on business requirements that summarise a number of access rights into typical user access profiles. Access requests and reviews are easier managed at the level of such roles than at the level of particular rights.

Consideration should be given to including clauses in personnel contracts and service contracts that specify sanctions if unauthorised access is attempted by personnel or contractors.

9.2.3 Management of privileged access rights

a) Control

The allocation and use of privileged access rights should be restricted and controlled.

b) Implementation guidance

The allocation of privileged access rights should be controlled through a formal authorisation process in accordance with the relevant access control policy. The following steps should be considered:

i) the privileged access rights associated with each system or process, e.g. operating system, database management system and each application and the users to whom they need to be allocated should be identified;

ii) privileged access rights should be allocated to users on a need-to-use basis and on an event by event basis in line with the access control policy, i.e. based on the minimum requirement for their functional roles;

iii) an authorisation process and a record of all privileges allocated should be maintained. Privileged access rights should not be granted until the authorisation process is complete;

iv) requirements for expiry of privileged access rights should be defined;

v) privileged access rights should be assigned to a user ID different from those used for regular business activities. Regular business activities should not be performed from privileged ID;

vi) the competences of users with privileged access rights should be reviewed regularly in order to verify if they are in line with their duties;

vii) specific procedures should be established and maintained in order to avoid the unauthorised use of generic administration user IDs, according to systems' configuration capabilities; and

viii) for generic administration user IDs, the confidentiality of secret authentication information should be maintained when shared (e.g. changing passwords frequently and as soon as possible when a privileged user leaves or changes job, communicating them among privileged users with appropriate mechanisms).

c) Other information

Inappropriate use of system administration privileges (any feature or facility of an information system that enables the user to override system or application controls) is a major contributory factor to failures or breaches of systems.

9.2.4 Management of secret authentication information of users

a) Control

The allocation of secret authentication information should be controlled through a formal management process.

b) Implementation guidance

The process should include the following requirements:

i) users should be required to sign a statement to keep personal secret authentication information confidential and to keep group (e.g. shared) secret authentication information solely within the members of the group; this signed statement may be included in the terms and conditions of employment;

ii) when users are required to maintain their own secret authentication information they should be provided initially with secure temporary secret authentication information`, which they are forced to change on first use;

iii) procedures should be established to verify the identity of a user prior to providing new, replacement or temporary secret authentication information;

iv) temporary secret authentication information should be given to users in a secure manner; the use of external party or unprotected (clear text) electronic mail messages should be avoided;

v) temporary secret authentication information should be unique to an individual and should not be guessable;

vi) users should acknowledge receipt of secret authentication information; and

vii) default vendor secret authentication information should be altered following installation of systems or software.

c) Other information

Passwords are a commonly used type of secret authentication information and are a common means of verifying a user's identity. Other types of secret authentication information are cryptographic keys and other data stored on hardware tokens (e.g. smart cards) that produce authentication codes.

9.2.5 Review of user access rights

a) Control

Asset owners should review users' access rights at regular intervals.

b) Implementation guidance

The review of access rights should consider the following:

i) users' access rights should be reviewed at regular intervals and after any changes, such as promotion, demotion or termination of employment;

ii) user access rights should be reviewed and re-allocated when moving from one role to another within the same organisation;

iii) authorisations for privileged access rights should be reviewed at more frequent intervals;

iv) privilege allocations should be checked at regular intervals to ensure that unauthorised privileges have not been obtained; and

v) changes to privileged accounts should be logged for periodic review.

c) Other information

This control compensates for possible weaknesses in the execution of clause 9.2.1, 9.2.2 and 9.2.6.

9.2.6 Removal or adjustment of access rights

a) Control

The access rights of all employees and external party users to information and information processing facilities should be removed upon termination of their employment, contract or agreement, or adjusted upon change.

b) Implementation guidance

Upon termination, the access rights of an individual to information and assets associated with information processing facilities and services should be removed or suspended. This will determine whether it is necessary to remove access rights. Changes of employment should be reflected in removal of all access rights that were not approved for the new employment. The access rights that should be removed or adjusted include those of physical and logical access. Removal or adjustment can be done by removal, revocation or replacement of keys, ID cards, information processing facilities or subscriptions. Any documentation that identifies access rights of employees and contractors should reflect the removal or adjustment of access rights. If a departing employee or external party user has known passwords for user IDs remaining active, these should be changed upon termination or change of employment, contract or agreement.

Access rights for information and assets associated with information processing facilities should be reduced or removed before the employment terminates or changes, depending on the evaluation of risk factors such as:

i) whether the termination or change is initiated by the employee, the external party user or by management, and the reason for termination;

ii) the current responsibilities of the employee, external party user or any other user; and

iii) the value of the assets currently accessible.

c) Other information

In certain circumstances access rights may be allocated on the basis of being available to more people than the departing employee or external party user, e.g. group IDs. In such circumstances, departing individuals should be removed from any group access lists and arrangements should be made to advise all other employees and external party users involved to no longer share this information with the person departing.

In cases of management initiated termination, disgruntled employees or external party users can deliberately corrupt information or sabotage information processing facilities. In cases of persons resigning or being dismissed, they may be tempted to collect information for future use.

9.3 User responsibilities

To make users accountable for safeguarding their authentication information.

9.3.1 Use of secret authentication information

a) Control

Users should be required to follow the organisation's practices in the use of secret authentication information.

b) Implementation guidance

All users should be advised to:

i) keep secret authentication information confidential, ensuring that it is not disclose to any other party, including people of authority;

ii) avoid keeping a record (e.g. on paper, software file or hand held device) of secret authentication information, unless this can be stored securely and the method of storing has been approved (e.g. password vault);

iii) change secret authentication information whenever there is any indication of its possible compromise;

iv) when passwords are used as secret authentication information, select quality passwords with sufficient minimum length which are:

1) easy to remember;

2) not based on anything somebody else could easily guess or obtain using person related information, e.g. names, telephone numbers and dates of birth etc.;

3) not vulnerable to dictionary attacks (i.e. do not consist of words included in dictionaries);

4) free of consecutive identical, all numeric or all alphabetic characters; and

5) if temporary, changed at the first log-on.

v) not share individual user's secret authentication information;

vi) ensure proper protection of passwords when passwords are used as secret authentication information in automated log-on procedures and are stored; and

vii) not use the same secret authentication information for business and non-business purposes.

c) Other information

Provision of Single Sign On (SSO) or other secret authentication information management tools reduces the amount of secret authentication information that users are required to protect and thus can increase the effectiveness of this control. However, these tools can also increase the impact of disclosure of secret authentication information.

9.4 System and application access control

To prevent unauthorised access to systems and applications.

9.4.1 Information access restriction

a) Control

Access to information and application system functions should be restricted in accordance with the access control policy.

b) Implementation guidance

Restrictions to access should be based on individual business application requirements and in accordance with the defined access control policy.

The following should be considered in order to support access restriction requirements:

i) providing menus to control access to application system functions;

ii) controlling which data can be accessed by a particular user;

iii) controlling the access rights of users, e.g. read, write, delete and execute;

iv) controlling the access rights of other applications;

v) limiting the information contained in outputs; and

vi) providing physical or logical access controls for the isolation of sensitive applications, application data, or systems.

9.4.2 Secure log-on procedures

a) Control

Where required by the access control policy, access to systems and applications should be controlled by a secure log-on procedure.

b) Implementation guidance

A suitable authentication technique should be chosen to substantiate the claimed identity of a user.

Where strong authentication and identity verification is required, authentication methods alternative to passwords, such as cryptographic means, smart cards, tokens or biometric means, should be used.

The procedure for logging into a system or application should be designed to minimise the opportunity for unauthorised access. The log-on procedure should therefore disclose the minimum of information about the system or application, in order to avoid providing an unauthorised user with any unnecessary assistance. A good log-on procedure should:

i) not display system or application identifiers until the log-on process has been successfully completed;

ii) display a general notice warning that the computer should only be accessed by authorised users;

iii) not provide help messages during the log-on procedure that would aid an unauthorised user;

iv) validate the log-on information only on completion of all input data. If an error condition arises, the system should not indicate which part of the data is correct or incorrect;

v) protect against brute force log-on attempts;

vi) log unsuccessful and successful attempts;

vii) raise a security event if a potential attempted or successful breach of log-on controls is detected;

viii) display the following information on completion of a successful log-on:

1) date and time of the previous successful log-on; and

2) details of any unsuccessful log-on attempts since the last successful log-on.

ix) not display a password being entered;

x) not transmit passwords in clear text over a network;

xi) terminate inactive sessions after a defined period of inactivity, especially in high risk locations such as public or external areas outside the organisation's security management or on mobile devices; and

xii) restrict connection times to provide additional security for high risk applications and reduce the window of opportunity for unauthorised access.

c) Other information

Passwords are a common way to provide ID and authentication based on a secret that only the user knows. The same can also be achieved with cryptographic means and authentication protocols. The strength of user authentication should be appropriate for the classification of the information to be accessed.

If passwords are transmitted in clear text during the log-on session over a network, they can be captured by a network "sniffer" program.

9.4.3 Password management system

a) Control

Password management systems should be interactive and should ensure quality passwords.

b) Implementation guidance

A password management system should:

i) enforce the use of individual user IDs and passwords to maintain accountability;

ii) allow users to select and change their own passwords and include a confirmation procedure to allow for input errors;

iii) enforce a choice of quality passwords;

iv) force users to change their passwords at the first log-on;

v) enforce regular password changes and as needed;

vi) maintain a record of previously used passwords and prevent re-use;

vii) not display passwords on the screen when being entered;

viii) store password files separately from application system data; and

ix) store and transmit passwords in protected form.

c) Other information

Some applications require user passwords to be assigned by an independent authority; in such cases, points ii), iv) and v) of the above guidance do not apply. In most cases the passwords are selected and maintained by users.

9.4.4 Use of privileged utility programs

a) Control

The use of utility programs that might be capable of overriding system and application controls should be restricted and tightly controlled.

b) Implementation guidance

The following guidelines for the use of utility programs that might be capable of overriding system and application controls should be considered:

i) use of ID, authentication and authorisation procedures for utility programs;

ii) segregation of utility programs from applications software;

iii) limitation of the use of utility programs to the minimum practical number of trusted, authorised users;

iv) authorisation for ad hoc use of utility programs;

v) limitation of the availability of utility programs, e.g. for the duration of an authorised change;

vi) logging of all use of utility programs;

vii) defining and documenting of authorisation levels for utility programs;

viii) removal or disabling of all unnecessary utility programs; and

ix) not making utility programs available to users who have access to applications on systems where segregation of duties is required.

c) Other information

Most computer installations have one or more utility programs that might be capable of overriding system and application controls.

9.4.5 Access control to program source code

a) Control

Access to program source code should be restricted.

b) Implementation guidance

Access to program source code and associated items (e.g. designs, specifications, verification plans and validation plans) should be strictly controlled, in order to prevent the introduction of unauthorised functionality and to avoid unintentional changes as well as to maintain the confidentiality of valuable intellectual property. For program source code, this can be achieved by controlled central storage of such code, preferably in program source libraries. The following guidelines should then be considered to control access to such program source libraries in order to reduce the potential for corruption of computer programs:

i) where possible, program source libraries should not be held in operational systems;

ii) the program source code and the program source libraries should be managed according to established procedures;

iii) support personnel should not have unrestricted access to program source libraries;

iv) the updating of program source libraries and associated items and the issuing of program sources to programmers should only be performed after appropriate authorisation has been received;

v) program listings should be held in a secure environment;

vi) an audit log should be maintained of all accesses to program source libraries; and

vii) maintenance and copying of program source libraries should be subject to strict change control procedures.

If the program source code is intended to be published, additional controls to help getting assurance on its integrity (e.g. digital signature) should be considered.

10. Cryptography

10.1 Cryptographic controls

To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.

10.1.1 Policy on the use of cryptographic controls

a) Control

A policy on the use of cryptographic controls for protection of information should be developed and implemented.

b) Implementation guidance

When developing a cryptographic policy, the following should be considered:

i) the management approach towards the use of cryptographic controls across the organisation, including the general principles under which business information should be protected;

ii) based on a risk assessment, the required level of protection should be identified taking into account the type, strength and quality of the encryption algorithm required;

iii) the use of encryption for protection of information transported by mobile or removable media devices or across communication lines;

iv) the approach to key management, including methods to deal with the protection of cryptographic keys and the recovery of encrypted information in the case of lost, compromised or damaged keys;

v) roles and responsibilities, e.g. who is responsible for:
   1) the implementation of the policy; and

   2) the key management, including key generation.

vi) the standards to be adopted for effective implementation throughout the organisation (which solution is used for which business processes); and

vii) the impact of using encrypted information on controls that rely upon content inspection (e.g. malware detection).

When implementing the organisation's cryptographic policy, consideration should be given to the regulations and national restrictions that might apply to the use of cryptographic techniques in different parts of the world and to the issues of trans border flow of encrypted information.

Cryptographic controls can be used to achieve different information security objectives:

i) Confidentiality

Using encryption of information to protect sensitive or critical information, either stored or transmitted.

ii) Integrity/Authenticity

Using digital signatures or message authentication codes to verify the authenticity or integrity of stored or transmitted sensitive or critical information.

iii) Non-repudiation

Using cryptographic techniques to provide evidence of the occurrence or non-occurrence of an event or action.

iv) Authentication

Using cryptographic techniques to authenticate users and other system entities requesting access to or transacting with system users, entities and resources.

c) Other information

Making a decision as to whether a cryptographic solution is appropriate should be seen as part of the wider process of risk assessment and selection of controls. This assessment can then be used to determine whether a cryptographic control is appropriate, what type of control should be applied and for what purpose and business processes.

A policy on the use of cryptographic controls is necessary to maximise the benefits and minimise the risks of using cryptographic techniques and to avoid inappropriate or incorrect use.

Specialist advice should be sought in selecting appropriate cryptographic controls to meet the information security policy objectives.

10.1.2 Key management

a) Control

A policy on the use, protection and lifetime of cryptographic keys should be developed and implemented through their whole lifecycle.

b) Implementation guidance

The policy should include requirements for managing cryptographic keys though their whole lifecycle including generating, storing, archiving, retrieving, distributing, retiring and destroying keys.

Cryptographic algorithms, key lengths and usage practices should be selected according to best practice. Appropriate key management requires secure processes for generating, storing, archiving, retrieving, distributing, retiring and destroying cryptographic keys.

All cryptographic keys should be protected against modification and loss. In addition, secret and private keys need protection against unauthorised use as well as disclosure. Equipment used to generate, store and archive keys should be physically protected.

A key management system should be based on an agreed set of standards, procedures and secure methods for:

i) generating keys for different cryptographic systems and different applications;

ii) issuing and obtaining public key certificates;

iii) distributing keys to intended entities, including how keys should be activated when received;

iv) storing keys, including how authorised users obtain access to keys;

v) changing or updating keys including rules on when keys should be changed and how this will be done;

vi) dealing with compromised keys;

vii) revoking keys including how keys should be withdrawn or deactivated, e.g. when keys have been compromised or when a user leaves an organisation (in which case keys should also be archived);

viii) recovering keys that are lost or corrupted;

ix) backing up or archiving keys;

x) destroying keys; and

xi) logging and auditing of key management related activities.

In order to reduce the likelihood of improper use, activation and deactivation dates for keys should be defined so that the keys can only be used for the period of time defined in the associated key management policy.

In addition to securely managing secret and private keys, the authenticity of public keys should also be considered. This authentication process can be done using public key certificates, which are normally issued by a certification authority, which should be a recognised organisation with suitable controls and procedures in place to provide the required degree of trust.

The contents of Service Level Agreement (SLA)s or contracts with external suppliers of cryptographic services, e.g. with a certification authority, should cover issues of liability, reliability of services and response times for the provision of services.

c) Other information

The management of cryptographic keys is essential to the effective use of cryptographic techniques. ISO/IEC 11770 provides further information on key management.

Cryptographic techniques can also be used to protect cryptographic keys. Procedures may need to be considered for handling legal requests for access to cryptographic keys, e.g. encrypted information can be required to be made available in an unencrypted form as evidence in a court case.

11. Physical and environmental security

11.1 Secure areas

To prevent unauthorised physical access, damage and interference to the organisation's information and information processing facilities.

11.1.1 Physical security perimeter

a) Control

Security perimeters should be defined and used to protect areas that contain sensitive or critical information, and information processing facilities.

b) Implementation guidance

The following guidelines should be considered and implemented where appropriate for physical security perimeters:

i) security perimeters should be defined, and the siting and strength of each of the perimeters should depend on the security requirements of the assets within the perimeter and the results of a risk assessment;

ii) perimeters of a building or site containing information processing facilities should be physically sound (i.e. there should be no gaps in the perimeter or areas where a break-in could easily occur); the exterior roof, walls and flooring of the site should be of solid construction and all external doors should be suitably protected against unauthorised access with control mechanisms, (e.g. bars, alarms, locks); doors and windows should be locked when unattended and external protection should be considered for windows, particularly at ground level;

iii) a manned reception area or other means to control physical access to the site or building should be in place; access to sites and buildings should be restricted to authorised personnel only;

iv) physical barriers should, where applicable, be built to prevent unauthorised physical access and environmental contamination;

v) all fire doors on a security perimeter should be alarmed, monitored and tested in conjunction with the walls to establish the required level of resistance in accordance with suitable regional, national and international standards; they should operate in accordance with the local fire code in a failsafe manner;

vi) suitable intruder detection systems should be installed to national, regional or international standards and regularly tested to cover all external doors and accessible windows; unoccupied areas should be alarmed at all times; cover should also be provided for other areas, e.g. computer room or communications rooms; and

vii) information processing facilities managed by the organisation should be physically separated from those managed by external party.

c) Broadcasting-specific implementation guidance

Broadcasting organisations should consider and implement the following guidelines where appropriate for physical security perimeters:

i) Broadcasting operations centres should be equipped with adequate physical intruder detection systems;

ii) facilities for broadcasting services, e.g. transmission facilities, switching facilities and broadcasting infrastructure, should be physically separated and sited away from other facilities, e.g. customer facilities in managed data centres; and

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

11.1.2 Physical entry controls

a) Control

Secure areas should be protected by appropriate entry controls to ensure that only authorised personnel are allowed access.

b) Implementation guidance

The following guidelines should be considered:

i) the date and time of entry and departure of visitors should be recorded, and all visitors should be supervised unless their access has been previously approved; they should only be granted access for specific, authorised purposes and should be issued with instructions on the security requirements of the area and on emergency procedures. The identity of visitors should be authenticated by an appropriate means;

ii) access to areas where confidential information is processed or stored should be restricted to authorised individuals only by implementing appropriate access controls, e.g. by implementing a two (2) factor authentication mechanism such as:

1) an access card; and

2) secret Personal Identification Number (PIN).

iii) a physical log book or electronic audit trail of all access should be securely maintained and monitored;

iv) all employees, contractors and external party should be required to wear some form of visible ID and should immediately notify security personnel if they encounter unescorted visitors and anyone not wearing visible ID;

v) external party support service personnel should be granted restricted access to secure areas or confidential information processing facilities only when required; this access should be authorised and monitored; and

vi) access rights to secure areas should be regularly reviewed and updated and revoked when necessary.

c) Broadcasting-specific implementation guidance

Broadcasting organisations should consider the following guidelines:

i) appropriate physical security controls should be applied to all broadcasting operation rooms and control centres;

ii) upon entry, relevant visitor data should be recorded and adequately protected from unauthorised disclosure; and

iii) visitor records should be physically and electronically protected to preserve the confidentiality, integrity and availability of the information they contain.

11.1.3 Securing offices, rooms, and facilities

a) Control

Physical security for offices, rooms and facilities should be designed and applied.

b) Implementation guidance

The following guidelines should be considered to secure offices, rooms and facilities:

i) key facilities should be sited to avoid access by the public;
ii) where applicable, buildings should be unobtrusive and give minimum indication of their purpose, with no obvious signs, outside or inside the building, identifying the presence of information processing activities;

iii) facilities should be configured to prevent confidential information or activities from being visible and audible from the outside. Electromagnetic shielding should also be considered as appropriate; and

iv) directories and internal telephone books identifying locations of confidential information processing facilities should not be readily accessible to anyone unauthorised.

11.1.4 Protecting against external and environmental threats

a) Control

Physical protection against natural disasters, malicious attack or accidents should be designed and applied.

b) Implementation guidance

Specialist advice should be obtained on how to avoid damage from fire, flood, earthquake, explosion, civil unrest and other forms of natural or man-made disaster.

11.1.5 Working in secure areas

a) Control

Procedures for working in secure areas should be designed and applied.

b) Implementation guidance

The following guidelines should be considered:

i) personnel should only be aware of the existence of, or activities within, a secure area on a need-to-know basis;

ii) unsupervised working in secure areas should be avoided both for safety reasons and to prevent opportunities for malicious activities;

iii) vacant secure areas should be physically locked and periodically reviewed; and

iv) photographic, video, audio or other recording equipment, such as cameras in mobile devices, should not be allowed, unless authorised.

The arrangements for working in secure areas include controls for the employees and external party users working in the secure area and they cover all activities taking place in the secure area.

11.1.6 Delivery and loading areas

a) Control

Access points such as delivery and loading areas and other points where unauthorised persons could enter the premises should be controlled and, if possible, isolated from information processing facilities to avoid unauthorised access.

b) Implementation guidance

The following guidelines should be considered:

i) access to a delivery and loading area from outside of the building should be restricted to identified and authorised personnel;

ii) the delivery and loading area should be designed so that supplies can be loaded and unloaded without delivery personnel gaining access to other parts of the building;

iii) the external doors of a delivery and loading area should be secured when the internal doors are opened;

iv) incoming material should be inspected and examined for explosives, chemicals or other hazardous materials, before it is moved from a delivery and loading area;

v) incoming material should be registered in accordance with asset management procedures on entry to the site;

vi) incoming and outgoing shipments should be physically segregated, where possible; and

vii) incoming material should be inspected for evidence of tampering en route. If such tampering is discovered it should be immediately reported to security personnel.

11.2 Equipment

To prevent loss, damage, theft or compromise of assets and interruption to the organisation's operations.

11.2.1 Equipment siting and protection

a) Control

Equipment should be sited or protected to reduce the risks from environmental threats and hazards, as well as opportunities for unauthorised access.

b) Implementation guidance

The following guidelines should be considered:

i) equipment should be sited to minimise unnecessary access into work areas;

ii) information processing facilities handling sensitive data should be positioned carefully to reduce the risk of information being viewed by unauthorised persons during their use;

iii) storage facilities should be secured to avoid unauthorised access;

iv) items requiring special protection should be safeguarded to reduce the general level of protection required;

v) controls should be adopted to minimise the risk of potential physical and environmental threats, e.g. theft, fire, explosives, smoke, water (or water supply failure), dust, vibration, chemical effects, electrical supply interference, communications interference, electromagnetic radiation and vandalism;

vi) guidelines for eating, drinking and smoking in proximity to information processing facilities should be established;

vii) environmental conditions, such as temperature and humidity, should be monitored for conditions which could adversely affect the operation of information processing facilities;

viii) lightning protection should be applied to all buildings and lightning protection filters should be fitted to all incoming power and communications lines;

ix) the use of special protection methods, such as keyboard membranes, should be considered for equipment in industrial environments; and

x) equipment processing confidential information should be protected to minimise the risk of information leakage due to electromagnetic emanation.

c) Broadcasting-specific implementation guidance

If the systems of several organisations are sited in the same data centre as broadcasting facilities, the broadcasting organisation should implement appropriate measures to protect customers' information stored in their systems. Such systems should have additional security in place, e.g. by being located in a separate secured area.

11.2.2 Supporting utilities

a) Control

Equipment should be protected from power failures and other disruptions caused by failures in supporting utilities.

b) Implementation guidance

Supporting utilities (e.g. electricity, telecommunications, water supply, gas, sewage, ventilation and air conditioning) should:

i) conform to equipment manufacturer's specifications and local legal requirements;

ii) be appraised regularly for their capacity to meet business growth and interactions with other supporting utilities;

iii) be inspected and tested regularly to ensure their proper functioning;

iv) if necessary, be alarmed to detect malfunctions; and

v) if necessary, have multiple feeds with diverse physical routing.

Emergency lighting and communications should be provided. Emergency switches and valves to cut off power, water, gas or other utilities should be located near emergency exits or equipment rooms.

c) Broadcasting-specific implementation guidance

In particular, power supply facilities in isolated areas, such as transmitter stations, should preferably provide an uninterruptible power supply with capacity for all loading and capable of withstanding primary power supply failures for the duration of likely outages. If that is impossible, a mechanism to provide uninterruptible power supply to critical equipment should be installed. Batteries may need to be augmented with a private electric generator, especially in isolated areas.

Any equipment room should have adequate Heating, Ventilation and Air Conditioning (HVAC) services to ensure external environmental conditions do not result in equipment operating outside manufacturers' guidelines.

d) Other information for broadcasting

Broadcasting organisations should specify in the agreement that supporting utilities are properly maintained and continually provided, in order to ensure the provision of broadcasting services without interruption.

11.2.3 Cabling security

a) Control

Power and broadcasting cabling carrying data or supporting information services should be protected from interception, interference or damage.

b) Implementation guidance

The following guidelines for cabling security should be considered:

i) power and telecommunications lines into information processing facilities should be underground, where possible, or subject to adequate alternative protection;

ii) power cables should be segregated from communications cables to prevent interference; and

iii) for sensitive or critical systems further controls to consider include:

1) installation of armoured conduit and locked rooms or boxes at inspection and termination points;

2) use of electromagnetic shielding to protect the cables;

3) initiation of technical sweeps and physical inspections for unauthorised devices being attached to the cables; and

4) controlled access to patch panels and cable rooms.

11.2.4 Equipment maintenance

a) Control

Equipment should be correctly maintained to ensure its continued availability and integrity.

b) Implementation guidance

The following guidelines for equipment maintenance should be considered:

i) equipment should be maintained in accordance with the supplier's recommended service intervals and specifications;

ii) only authorised maintenance personnel should carry out repairs and service equipment;

iii) records should be kept of all suspected or actual faults, and of all preventive and corrective maintenance;

iv) appropriate controls should be implemented when equipment is scheduled for maintenance, taking into account whether this maintenance is performed by personnel on site or external to the organisation; where necessary, confidential information should be cleared from the equipment or the maintenance personnel should be sufficiently cleared;

v) all maintenance requirements imposed by insurance policies should be complied with; and

vi) before putting equipment back into operation after its maintenance, it should be inspected to ensure that the equipment has not been tampered with and does not malfunction.

11.2.5 Removal of assets

a) Control

Equipment, information or software should not be taken off-site without prior authorisation.

b) Implementation guidance

The following guidelines should be considered:

i) employees and external party users who have authority to permit off-site removal of assets should be identified;

ii) time limits for asset removal should be set and returns verified for compliance;

iii) where necessary and appropriate, assets should be recorded as being removed off-site and recorded when returned; and

iv) the identity, role and affiliation of anyone who handles or uses assets should be documented and this documentation returned with the equipment, information or software.

c) Other information

Spot checks, undertaken to detect unauthorised removal of assets, can also be performed to detect unauthorised recording devices, weapons, etc., and to prevent their entry into and exit from, the site. Such spot checks should be carried out in accordance with relevant legislation and regulations. Individuals should be made aware that spot checks are carried out, and the verifications should only be performed with authorisation appropriate for the legal and regulatory requirements.

11.2.6 Security of equipment and assets off-premises

a) Control

Security should be applied to off-site assets taking into account the different risks of working outside the organisation's premises.

b) Implementation guidance

The use of any information storing and processing equipment outside the organisation's premises should be authorised by management. This applies to equipment owned by the organisation and that equipment owned privately and used on behalf of the organisation.

The following guidelines should be considered for the protection of off-site equipment:

i) equipment and media taken off premises should not be left unattended in public places;

ii) manufacturers' instructions for protecting equipment should be observed at all times, e.g. protection against exposure to strong electromagnetic fields;

iii) controls for off-premises locations, such as home working, teleworking and temporary sites should be determined by a risk assessment and suitable controls applied as appropriate, e.g. lockable filing cabinets, clear desk policy, access controls for computers and secure communication with the office; and

iv) when off-premises equipment is transferred among different individuals or external party, a log should be maintained that defines the chain of custody for the equipment including at least names and organisations of those who are responsible for the equipment.

Risks, e.g. of damage, theft or eavesdropping, may vary considerably between locations and should be taken into account in determining the most appropriate controls.

11.2.7 Secure disposal or re-use of equipment

a) Control

All items of equipment containing storage media should be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.

b) Implementation guidance

Equipment should be verified to ensure whether or not storage media is contained prior to disposal or re-use.

Storage media containing confidential or copyrighted information should be physically destroyed or the information should be destroyed, deleted or overwritten using techniques to make the original information non-retrievable rather than using the standard delete or format function.

c) Other information

Damaged equipment containing storage media may require a risk assessment to determine whether the items should be physically destroyed rather than sent for repair or discarded. Information can be compromised through careless disposal or re-use of equipment.

In addition to secure disk erasure, whole disk encryption reduces the risk of disclosure of confidential information when equipment is disposed of or redeployed, provided that:

i) the encryption process is sufficiently strong and covers the entire disk (including slack space, swap files, etc.);

ii) the encryption keys are long enough to resist brute force attacks; and

iii) the encryption keys are themselves kept confidential (e.g. never stored on the same disk).

For further advice on encryption, see Clause 10.

Techniques for securely overwriting storage media differ according to the storage media technology. Overwriting tools should be reviewed to make sure that they are applicable to the technology of the storage media.

11.2.8 Unattended user equipment

a) Control

Users should ensure that unattended equipment has appropriate protection.

b) Implementation guidance

All users should be made aware of the security requirements and procedures for protecting unattended equipment, as well as their responsibilities for implementing such protection. Users should be advised to:

i) terminate active sessions when finished, unless they can be secured by an appropriate locking mechanism, e.g. a password protected screen saver;

ii) log-off from applications or network services when no longer needed; and

iii) secure computers or mobile devices from unauthorised use by a key lock or an equivalent control, e.g. password access, when not in use.

11.2.9 Clear desk and clear screen policy

a) Control

A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities should be adopted.

b) Implementation guidance

The clear desk and clear screen policy should take into account the information classifications, legal and contractual requirements and the corresponding risks and cultural aspects of the organisation. The following guidelines should be considered:

i) sensitive or critical business information, e.g. on paper or on electronic storage media, should be locked away (ideally in a safe or cabinet or other forms of security furniture) when not required, especially when the office is vacated;
ii) computers and terminals should be left logged off or protected with a screen and keyboard locking mechanism controlled by a password, token or similar user authentication mechanism when unattended and should be protected by key locks, passwords or other controls when not in use;

iii) unauthorised use of photocopiers and other reproduction technology (e.g. scanners, digital cameras) should be prevented; and

iv) media containing sensitive or classified information should be removed from printers immediately.

c) Other information

A clear desk/clear screen policy reduces the risks of unauthorised access, loss of and damage to information during and outside normal working hours. Safes or other forms of secure storage facilities might also protect information stored therein against disasters such as a fire, earthquake, flood or explosion.

Consider the use of printers with PIN code function, so the originators are the only ones who can get their print outs and only when standing next to the printer.

12. Operations security

12.1 Operational procedures and responsibilities

To ensure correct and secure operations of information processing facilities.

12.1.1 Documented operating procedures

a) Control

Operating procedures should be documented and made available to all users who need them.

b) Implementation guidance

Documented procedures should be prepared for operational activities associated with information processing and communication facilities, such as computer start up and close down procedures, backup, equipment maintenance, media handling, computer room and mail handling management and safety.

The operating procedures should specify the operational instructions, including:

i) the installation and configuration of systems;

ii) processing and handling of information both automated and manual;

iii) backup;

iv) scheduling requirements, including interdependencies with other systems, earliest job start and latest job completion times;

v) instructions for handling errors or other exceptional conditions, which might arise during job execution, including restrictions on the use of system utilities;

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

vii) special output and media handling instructions, such as the use of special stationery or the management of confidential output including procedures for secure disposal of output from failed jobs;

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

ix) the management of audit-trail and system log information; and

x) monitoring procedures.

c) Broadcasting-specific implementation guidance

In the operating procedures, broadcasting organisations should specify under which conditions the incident, emergency or crisis handling procedures are to be invoked.

Operating procedures and the documented procedures for system activities should be treated as formal documents and changes authorised by management. Where technically feasible, information systems should be managed consistently, using the same procedures, tools and utilities.

12.1.2 Change management

a) Control

Changes to the organisation, business processes, information processing facilities and systems that affect information security should be controlled.

b) Implementation guidance

In particular, the following items should be considered:

i) ID and recording of significant changes;

ii) planning and testing of changes;

iii) assessment of the potential impacts, including information security impacts, of such changes;

iv) formal approval procedure for proposed changes;

v) verification that information security requirements have been met;

vi) communication of change details to all relevant persons;

vii) fall back procedures, including procedures and responsibilities for aborting and recovering from unsuccessful changes and unforeseen events; and

viii) provision of an emergency change process to enable quick and controlled implementation of changes needed to resolve an incident.

Formal management responsibilities and procedures should be in place to ensure satisfactory control of all changes. When changes are made, an audit log containing all relevant information should be retained.

c) Broadcasting-specific implementation guidance

Inadequate control of changes to information processing facilities and systems is a common cause of system or security failures. Changes to the operational environment, especially when transferring system from development to operational stage, can impact the reliability of the broadcasting organisation's services.

In implementing a change management in broadcasting organisations, the following items should be considered:

i) the roles and responsibilities of the change process e.g. request and approval procedures, authorisations requirement;

ii) different types of change to accommodate different types of operating environment, e.g. normal change, critical change, emergency change;

iii) communications with relevant party such as employee, service subscriber, business partner, vendor and other broadcasting organisations on the changes and possible outcome from such changes;

iv) when handling changes, information such as types of change, justification of changes, possible impact if the changes fail, test result, fall-back plan, approval should be formally recorded;

v) compatibility with other software in use;

vi) testing of new software, configuration, system image in a segregated environment from production system if practical; and

vii) ensuring that the implementation of changes takes place at the right time and does not disturb the business processes involved.

d) Other information

Broadcasting organisations should consider the procedures and records for installation, relocation and removal of facilities. Changes to infrastructure, including both physical and logical modifications, should be subject to a change management process. When applicable, this process should seek approval from a designated risk owner. Output from the change process, including risk assessments, should be subject to regular security audits.

12.1.3 Capacity management

a) Control

The use of resources should be monitored, tuned and projection made of future capacity requirements to ensure the required system performance.

b) Implementation guidance

Capacity requirements should be identified, taking into account the business criticality of the concerned system. System tuning and monitoring should be applied to ensure and, where necessary, improve the availability and efficiency of systems. Detective controls should be put in place to indicate problems in due time. Projections of future capacity requirements should take account of new business and system requirements and current and projected trends in the organisation's information processing capabilities.

Particular attention needs to be paid to any resources with long procurement lead times or high costs, therefore managers should monitor the utilisation of key system resources. They should identify trends in usage, particularly in relation to business applications or information systems management tools. Managers should use this information to identify and avoid potential bottlenecks and dependence on key personnel that might present a threat to system security or services and plan appropriate action.

Providing sufficient capacity can be achieved by increasing capacity or by reducing demand. Examples of managing capacity demand include:

i) deletion of obsolete data (disk space);

ii) decommissioning of applications, systems, databases or environments;

iii) optimising batch processes and schedules;

iv) optimising application logic or database queries; and

v) denying or restricting bandwidth for resource-hungry services if these are not business critical (e.g. video streaming).

A documented capacity management plan should be considered for mission critical systems.

c) Broadcasting-specific implementation guidance

Capacity management should be used to avoid potential bottlenecks and achieve optimum performance of broadcasting organisation's services.

When planning for capacity management, considered the following:

i) capacity requirements (e.g. switching, network, computer, hardware, software, bandwidth, physical space, logical space, cabling, utilities, human resource etc.) should be identified, taking into account the business criticality and SLA with subscriber of the concerned system;

ii) threshold should be identified to trigger the warning on system capacity level and the mechanism and frequency of capacity management should be determined and approved by the management. Priority should be given to any resources with long procurement lead time or high costs;

iii) broadcasting organisations should have mechanism to detect network congestion and avoid the concentration of communications in case of network congestion;

iv) broadcasting organisations should recognise the performance limit of the relevant communication facilities and implement mechanism to control a number of communications requests before reaching the limits;

v) roles and responsibility for capacity management should be identified;

vi) for capacity management using IT tools, the accuracy of the information collected should be verified;

vii) resources usage trending should be identified and analysed align with the business requirement; and

viii) in the event that capacity expansion is not possible, prioritisation of services should be considered.

12.1.4 Separation of development, testing and operational environments

a) Control

Development, testing and operational environments should be separated to reduce the risks of unauthorised access or changes to the operational environment.

b) Implementation guidance

The level of separation between operational, testing, and development environments that is necessary to prevent operational problems should be identified and implemented.

The following items should be considered:

i) rules for the transfer of software from development to operational status should be defined and documented;

ii) development and operational software should run on different systems or computer processors and in different domains or directories;

iii) changes to operational systems and applications should be tested in a testing or staging environment prior to being applied to operational systems;

iv) other than in exceptional circumstances, testing should not be done on operational systems;

v) compilers, editors and other development tools or system utilities should not be accessible from operational systems when not required;

vi) users should use different user profiles for operational and testing systems, and menus should display appropriate ID messages to reduce the risk of error; and

vii) sensitive data should not be copied into the testing system environment unless equivalent controls are provided for the testing system.

c) Broadcasting-specific implementation guidance

In broadcasting organisations, the content of the data used in test and development environments should be adequate to test the system and service in a real broadcasting context. When the test data include sensitive information (e.g. PII and telephone records), appropriate controls should be implemented in order to avoid unintended information leakage caused by program bugs or operational errors.

In addition, such test data should be managed appropriately, taking account of data life cycle, such as collection of operation data including sensitive information, production of test data from operation data and destruction of test data after the test.

Wherever possible, non-operational data or anonymised data produced from operational data should be used for testing.

Development staff should only have access to operational passwords or other authentication tokens where controls are in place for temporary authorisation used for the support of operational systems.

Controls should ensure that such authorisations are revoked or authentication tokens are changed after use.

Testing should not be done on operational systems unless approved by the top management.

12.2 Protection from malware

To ensure that information and information processing facilities are protected against malware.

12.2.1 Controls against malware

a) Control

Detection, prevention and recovery controls to protect against malware should be implemented, combined with appropriate user awareness.

b) Implementation guidance

Protection against malware should be based on malware detection and repair software, information security awareness and appropriate system access and change management controls. The following guidance should be considered:

i) establishing a formal policy prohibiting the use of unauthorised software;

ii) implementing controls that prevent or detect the use of unauthorised software (e.g. application whitelisting);

iii) implementing controls that prevent or detect the use of known or suspected malicious websites (e.g. blacklisting);

iv) establishing a formal policy to protect against risks associated with obtaining files and software either from or via external networks or on any other medium, indicating what protective measures should be taken;

v) reducing vulnerabilities that could be exploited by malware, e.g. through technical vulnerability management;

vi) conducting regular reviews of the software and data content of systems supporting critical business processes; the presence of any unapproved files or unauthorised amendments should be formally investigated;

vii) installation and regular update of malware detection and repair software to scan computers and media as a precautionary control, or on a routine basis; the scan carried out should include:

1) scan any files received over networks or via any form of storage medium, for malware before use;

2) scan electronic mail attachments and downloads for malware before use; this scan should be carried out at different places, e.g. at electronic mail servers, desktop computers and when entering the network of the organisation; and

3) scan web pages for malware.

viii) defining procedures and responsibilities to deal with malware protection on systems, training in their use, reporting and recovering from malware attacks;

ix) preparing appropriate BCPs for recovering from malware attacks, including all necessary data and software backup and recovery arrangements;

x) implementing procedures to regularly collect information, such as subscribing to mailing lists or verifying websites giving information about new malware;

xi) implementing procedures to verify information relating to malware, and ensure that warning bulletins are accurate and informative; managers should ensure that qualified sources, e.g. reputable journals, reliable Internet sites or suppliers producing software protecting against malware, are used to differentiate between hoaxes and real malware; all users should be made aware of the problem of hoaxes and what to do on receipt of them; and

xii) isolating environments where catastrophic impacts may result.

c) Other information

The use of two or more software products protecting against malware across the information processing environment from different vendors and technology can improve the effectiveness of malware protection.

Care should be taken to protect against the introduction of malware during maintenance and emergency procedures, which may bypass normal malware protection controls.

Under certain conditions, malware protection might cause disturbance within operations.

Use of malware detection and repair software alone as a malware control is not usually adequate and commonly needs to be accompanied by operating procedures that prevent introduction of malware.

12.3 Backup

To protect against loss of data.

12.3.1 Information backup

a) Control

Backup copies of information, software and system images should be taken and tested regularly in accordance with an agreed backup policy.

b) Implementation guidance

A backup policy should be established to define the organisation's requirements for backup of information, software and systems.

The backup policy should define the retention and protection requirements.

Adequate backup facilities should be provided to ensure that all essential information and software can be recovered following a disaster or media failure.

When designing a backup plan, the following items should be taken into consideration:

i) accurate and complete records of the backup copies and documented restoration procedures should be produced;

ii) the extent (e.g. full or differential backup) and frequency of backups should reflect the business requirements of the organisation, the security requirements of the information involved and the criticality of the information to the continued operation of the organisation;

iii) the backups should be stored in a remote location, at a sufficient distance to escape any damage from a disaster at the main site;

iv) backup information should be given an appropriate level of physical and environmental protection consistent with the standards applied at the main site;

v) backup media should be regularly tested to ensure that they can be relied upon for emergency use when necessary; this should be combined with a test of the restoration procedures and checked against the restoration time required. Testing the ability to restore backed-up data should be performed onto dedicated test media, not by overwriting the original media in case the backup or restoration process fails and causes irreparable data damage or loss; and

vi) in situations where confidentiality is of importance, backups should be protected by means of encryption.

Operational procedures should monitor the execution of backups and address failures of scheduled backups to ensure completeness of backups according to the backup policy.

Backup arrangements for individual systems and services should be regularly tested to ensure that they meet the requirements of BCPs. In the case of critical systems and services, backup arrangements should cover all systems information, applications and data necessary to recover the complete system in the event of a disaster.

The retention period for essential business information should be determined, taking into account any requirement for archive copies to be permanently retained.

12.4 Logging and monitoring

To record events and generate evidence.

12.4.1 Event logging

a) Control

Event logs recording user activities, exceptions, faults and information security events should be produced, kept and regularly reviewed.

b) Implementation guidance

Event logs should include, when relevant:

i) user IDs;

ii) system activities;

iii) dates, times and details of key events, e.g. log-on and log-off;

iv) device identity or location if possible and system identifier;

v) records of successful and rejected system access attempts;

vi) records of successful and rejected data and other resource access attempts;

vii) changes to system configuration;

viii) use of privileges;

ix) use of system utilities and applications;

x) files accessed and the kind of access;

xi) network addresses and protocols;

xii) alarms raised by the access control system;

xiii) activation and de-activation of protection systems, such as anti-virus systems and intrusion detection systems; and

xiv) records of transactions executed by users in applications.

Event logging sets the foundation for automated monitoring systems which are capable of generating consolidated reports and alerts on system security.

c) Broadcasting-specific implementation guidance

Broadcasting organisations should set the appropriate retention time period for retaining data of broadcasting data (e.g. accounting, billing, attending to complaints, and protection of lawful access by the authorities) and delete the data at the end of the retention period or at the attainment of the purposes without any delay. This should be done in accordance to any business, legal and regulatory requirement that might apply.

12.4.2 Protection of log information

a) Control

Logging facilities and log information should be protected against tampering and unauthorised access.

b) Implementation guidance

Controls should aim to protect against unauthorised changes to log information and operational problems with the logging facility including:

i) alterations to the message types that are recorded;

ii) log files being edited or deleted; and

iii) storage capacity of the log file media being exceeded, resulting in either the failure to record events or overwriting of past recorded events.

Some audit logs may be required to be archived as part of the record retention policy or because of requirements to collect and retain evidence.

c) Other information

System logs often contain a large volume of information, much of which is extraneous to information security monitoring. To help identify significant events for information security monitoring purposes, the copying of appropriate message types automatically to a second log, or the use of suitable system utilities or audit tools to perform file interrogation and rationalisation should be considered.

System logs need to be protected, because if the data can be modified or data in them deleted, their existence may create a false sense of security. Real time copying of logs to a system outside the control of a system administrator or operator can be used to safeguard logs.

12.4.3 Administrator and operator logs

a) Control

System administrator and system operator activities should be logged and the logs protected and regularly reviewed.

b) Implementation guidance

Privileged user account holders may be able to manipulate the logs on information processing facilities under their direct control, therefore it is necessary to protect and review the logs to maintain accountability for the privileged users.

c) Other information

An intrusion detection system managed outside of the control of system and network administrators can be used to monitor system and network administration activities for compliance.

12.4.4 Clock synchronisation

a) Control

The clocks of all relevant information processing systems within an organisation or security domain should be synchronised to a single reference time source.

b) Implementation guidance

External and internal requirements for time representation, synchronisation and accuracy should be documented. Such requirements can be legal, regulatory, contractual requirements, standards compliance or requirements for internal monitoring. A standard reference time for use within the organisation should be defined.

The organisation's approach to obtaining a reference time from external source(s) and how to synchronise internal clocks reliably should be documented and implemented.

c) Other information

The correct setting of computer clocks is important to ensure the accuracy of audit logs, which may be required for investigations or as evidence in legal or disciplinary cases. Inaccurate audit logs may hinder such investigations and damage the credibility of such evidence. A clock linked to a radio time broadcast from a national atomic clock can be used as the master clock for logging systems. A network time protocol can be used to keep all of the servers in synchronisation with the master clock.

12.5 Control of operational software

To ensure the integrity of operational systems.

12.5.1 Installation of software on operational systems

a) Control

Procedures should be implemented to control the installation of software on operational systems.

b) Implementation guidance

The following guidelines should be considered to control changes of software on operational systems:

i) the updating of the operational software, applications and program libraries should only be performed by trained administrators upon appropriate management authorisation;

ii) operational systems should only hold approved executable code and not development code or compilers;

iii) applications and operating system software should only be implemented after extensive and successful testing; the tests should cover usability, security, effects on other systems and user friendliness and should be carried out on separate systems; it should be ensured that all corresponding program source libraries have been updated;

iv) a configuration control system should be used to keep control of all implemented software as well as the system documentation;

v) a rollback strategy should be in place before changes are implemented;

vi) an audit log should be maintained of all updates to operational program libraries;

vii) previous versions of application software should be retained as a contingency measure; and

viii) old versions of software should be archived, together with all required information and parameters, procedures, configuration details and supporting software for as long as the data are retained in archive.

Vendor supplied software used in operational systems should be maintained at a level supported by the supplier. Over time, software vendors will conclude to support older versions of software. The organisation should consider the risks of relying on unsupported software.

Any decision to upgrade to a new release should take into account the business requirements for the change and the security of the release, e.g. the introduction of new information security functionality or the number and severity of information security problems affecting this version. Software patches should be applied when they can help to remove or reduce information security weaknesses.

Physical or logical access should only be given to suppliers for support purposes when necessary and with management approval. The supplier’s activities should be monitored.

Computer software may rely on externally supplied software and modules, which should be monitored and controlled to avoid unauthorised changes, which could introduce security weaknesses.

c) Broadcasting-specific implementation guidance

Broadcasting organisations should minimise the risk of corruption to operational systems by considering the following guidelines to control changes:

i) changes to critical systems' applications or operating system software should be fully tested. Procedures for rolling back such an upgrade should be included;

ii) if application software is sensitive, then at least one generation of software should be retained;

iii) regression test of any updates, patches and changes on a test system, and ensure they operate correctly before they are implemented in an operational environment; and

iv) the changes of the software on operational system should be control via a proper change management procedure.

12.6 Technical vulnerability management

To prevent exploitation of technical vulnerabilities.

12.6.1 Management of technical vulnerabilities

a) Control

Information about technical vulnerabilities of information systems being used should be obtained in a timely fashion, the organisation's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.

b) Implementation guidance

A current and complete inventory of assets is a prerequisite for effective technical vulnerability management. Specific information needed to support technical vulnerability management includes the software vendor, version numbers, current state of deployment (e.g. what software is installed on what systems) and the person(s) within the organisation responsible for the software.

Appropriate and timely action should be taken in response to the ID of potential technical vulnerabilities. The following guidance should be followed to establish an effective management process for technical vulnerabilities:

i) the organisation should define and establish the roles and responsibilities associated with technical vulnerability management, including vulnerability monitoring, vulnerability risk assessment, patching, asset tracking and any coordination responsibilities required;

ii) information resources that will be used to identify relevant technical vulnerabilities and to maintain awareness about them should be identified for software and other technology (based on the asset inventory list); these information resources should be updated based on changes in the inventory or when other new or useful resources are found;

iii) a timeline should be defined to react to notifications of potentially relevant technical vulnerabilities;

iv) once a potential technical vulnerability has been identified, the organisation should identify the associated risks and the actions to be taken; such action could involve patching of vulnerable systems or applying other controls;

v) depending on how urgently a technical vulnerability needs to be addressed, the action taken should be carried out according to the controls related to change management or by following information security incident response procedures;

vi) if a patch is available from a legitimate source, the risks associated with installing the patch should be assessed (the risks posed by the vulnerability should be compared with the risk of installing the patch);

vii) patches should be tested and evaluated before they are installed to ensure they are effective and do not result in side effects that cannot be tolerated; if no patch is available, other controls should be considered, such as:

    1) turning off services or capabilities related to the vulnerability;

    2) adapting or adding access controls, e.g. firewalls, at network borders;

    3) increased monitoring to detect actual attacks; and

    4) raising awareness of the vulnerability.

viii) an audit log should be kept for all procedures undertaken;

ix) the technical vulnerability management process should be regularly monitored and evaluated in order to ensure its effectiveness and efficiency;

x) systems at high risk should be addressed first;

xi) an effective technical vulnerability management process should be aligned with incident management activities, to communicate data on vulnerabilities to the incident response function and provide technical procedures to be carried out should an incident occur; and

xii) define a procedure to address the situation where a vulnerability has been identified but there is no suitable countermeasure. In this situation, the organisation should evaluate risks relating to the known vulnerability and define appropriate detective and corrective actions.

12.6.2 Restrictions on software installation

a) Control

Rules governing the installation of software by users should be established and implemented.

b) Implementation guidance

The organisation should define and enforce strict policy on which types of software users may install.

The principle of least privilege should be applied. If granted certain privileges, users may have the ability to install software. The organisation should identify what types of software installations are permitted (e.g. updates and security patches to existing software) and what types of installations are prohibited (e.g. software that is only for personal use and software whose pedigree with regard to being potentially malicious is unknown or suspect). These privileges should be granted having regard to the roles of the users concerned.

c) Broadcasting-specific implementation guidance

For sensitive systems such as network elements or operations systems, only verified and permitted software should be installed.

Only authorised maintenance personnel should be able to install software on sensitive systems. This restriction should also be applied on the terminals used to administer the sensitive systems.

Software that can adversely affect sensitive systems performance and/or security should be controlled and monitored.

12.7 Information systems audit considerations

To minimise the impact of audit activities on operational systems.

12.7.1 Information systems audit controls

a) Control

Audit requirements and activities involving verification of operational systems should be carefully planned and agreed to minimise disruptions to business processes.

b) Implementation guidance

The following guidelines should be observed:

i) audit requirements for access to systems and data should be agreed with appropriate management;

ii) the scope of technical audit tests should be agreed and controlled;

iii) audit tests should be limited to read-only access to software and data;

iv) access other than read-only should only be allowed for isolated copies of system files, which should be erased when the audit is completed, or given appropriate protection if there is an obligation to keep such files under audit documentation requirements;

v) requirements for special or additional processing should be identified and agreed;

vi) audit tests that could affect system availability should be run outside business hours; and

vii) all access should be monitored and logged to produce a reference trail.

13. Communications security

13.1 Network security management

To ensure the protection of information in networks and its supporting information processing facilities.

13.1.1 Network controls

a) Control

Networks should be managed and controlled to protect information in systems and applications.

b) Implementation guidance

Controls should be implemented to ensure the security of information in networks and the protection of connected services from unauthorised access. In particular, the following items should be considered:

i) responsibilities and procedures for the management of networking equipment should be established;

ii) operational responsibility for networks should be separated from computer operations where appropriate;

iii) special controls should be established to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks and to protect the connected systems and applications; special controls may also be required to maintain the availability of the network services and computers connected;

iv) appropriate logging and monitoring should be applied to enable recording and detection of actions that may affect, or are relevant to, information security;

v) management activities should be closely coordinated both to optimise the service to the organisation and to ensure that controls are consistently applied across the information processing infrastructure;

vi) systems on the network should be authenticated; and

vii) systems connection to the network should be restricted.

c) Other information

Additional information on network security can be found in ISO/IEC 27033.

13.1.2 Security of network services

a) Control

Security mechanisms, service levels and management requirements of all network services should be identified and included in network services agreement, whether these services are provided in house or outsourced.

b) Implementation guidance

The ability of the network service provider to manage agreed services in a secure way should be determined and regularly monitored, and the right to audit should be agreed.

The security arrangements necessary for particular services, such as security features, service levels and management requirements, should be identified. The organisation should ensure that network service providers implement these measures.

13.1.3 Segregation in networks

a) Control

Groups of information services, users and information systems should be segregated on networks.

b) Implementation guidance

One method of managing the security of large networks is to divide them into separate network domains. The domains can be chosen based on trust levels (e.g. public access domain, desktop domain, server domain), along organisational units (e.g. human resources, finance, marketing) or some combination (e.g. server domain connecting to multiple organisational units). The segregation can be done using either physically different networks or by using different logical networks (e.g. VPN).

The perimeter of each domain should be well defined. Access between network domains is allowed, but should be controlled at the perimeter using a gateway (e.g. firewall, filtering router). The criteria for segregation of networks into domains, and the access allowed through the gateways, should be based on an assessment of the security requirements of each domain. The assessment should be in accordance with the access control policy, access requirements, value and classification of information processed and also take account of the relative cost and performance impact of incorporating suitable gateway technology.

Wireless networks require special treatment due to the poorly defined network perimeter. For sensitive environments, consideration should be made to treat all wireless access as external connections and to segregate this access from internal networks until the access has passed through a gateway in accordance with network controls policy before granting access to internal systems.

The authentication, encryption and user level network access control technologies of modern, standards based wireless networks may be sufficient for direct connection to the organisation’s internal network when properly implemented.

c) Broadcasting-specific implementation guidance

Specific attention should be given to segregate broadcast and management networks.

13.2 Information transfer

To maintain the security of information transferred within an organisation and with any external entity.

13.2.1 Information transfer policies and procedures

a) Control

Formal transfer policies, procedures and controls should be in place to protect the transfer of information through the use of all types of communication facilities.

b) Implementation guidance

The procedures and controls to be followed when using communication facilities for information transfer should consider the following items:

i) procedures designed to protect transferred information from interception, copying, modification, mis-routing and destruction;

ii) procedures for the detection of and protection against malware that may be transmitted through the use of electronic communications;

iii) procedures for protecting communicated sensitive electronic information that is in the form of an attachment;

iv) policy or guidelines outlining acceptable use of communication facilities;

v) personnel, external party and any other user's responsibilities not to compromise the organisation, e.g. through defamation, harassment, impersonation, forwarding of chain letters, unauthorised purchasing, etc.;

vi) use of cryptographic techniques e.g. to protect the confidentiality, integrity and authenticity of information (see Clause 10);

vii) retention and disposal guidelines for all business correspondence, including messages, in accordance with relevant national and local legislation and regulations;

viii) controls and restrictions associated with using communication facilities, e.g. automatic forwarding of electronic mail to external mail addresses;

ix) advising personnel to take appropriate precautions not to reveal confidential information;

x) not leaving messages containing confidential information on answering machines since these may be replayed by unauthorised persons, stored on communal systems or stored incorrectly as a result of misdialling; and

xi) advising personnel about the problems of using facsimile machines or services, namely:

1) unauthorised access to built-in message stores to retrieve messages;

2) deliberate or accidental programming of machines to send messages to specific numbers; and

3) sending documents and messages to the wrong number either by mis-dialling or using the wrong stored number.

In addition, personnel should be reminded that they should not have confidential conversations in public places or over insecure communication channels, open offices and meeting places.

Information transfer services should comply with any relevant legal requirements.

c) Other information

Information transfer may occur through the use of a number of different types of communication facilities, including electronic mail, voice, facsimile and video.

Software transfer may occur through a number of different mediums, including downloading from the Internet and acquisition from vendors selling off-the-shelf products.
The business, legal and security implications associated with electronic data interchange, electronic commerce and electronic communications and the requirements for controls should be considered.

13.2.2 Agreements on information transfer

a) Control

Agreements should address the secure transfer of business information between the organisation and external party.

b) Implementation guidance

Information transfer agreements should incorporate the following:

i) management responsibilities for controlling and notifying transmission, dispatch and receipt;

ii) procedures to ensure traceability and non-repudiation;

iii) minimum technical standards for packaging and transmission;

iv) escrow agreements;

v) courier ID standards;

vi) responsibilities and liabilities in the event of information security incidents, such as loss of data;

vii) use of an agreed labelling system for sensitive or critical information, ensuring that the meaning of the labels is immediately understood and that the information is appropriately protected;

viii) technical standards for recording and reading information and software;

ix) any special controls that are required to protect sensitive items, such as cryptography (see Clause 10);

x) maintaining a chain of custody for information while in transit; and

xi) acceptable levels of access control.

Policies, procedures and standards should be established and maintained to protect information and physical media in transit and should be referenced in such transfer agreements.
The information security content of any agreement should reflect the sensitivity of the business information involved.

c) Other information

Agreements may be electronic or manual and may take the form of formal contracts. For confidential information, the specific mechanisms used for the transfer of such information should be consistent for all organisations and types of agreements.

13.2.3 Electronic messaging

a) Control

Information involved in electronic messaging should be appropriately protected.

b) Implementation guidance

Information security considerations for electronic messaging should include the following:

i) protecting messages from unauthorised access, modification or denial of service commensurate with the classification scheme adopted by the organisation;

ii) ensuring correct addressing and transportation of the message;

iii) reliability and availability of the service;

iv) legal considerations, for example requirements for electronic signatures;

v) obtaining approval prior to using external public services such as instant messaging, social networking or file sharing; and

vi) stronger levels of authentication controlling access from publicly accessible networks.

c) Other information

There are many types of electronic messaging such as email, electronic data interchange and social networking which play a role in business communications.

13.2.4 Confidentiality or non-disclosure agreements

a) Control

Requirements for confidentiality or non-disclosure agreements reflecting the organisation's needs for the protection of information should be identified, regularly reviewed and documented.

b) Implementation guidance

Confidentiality or non-disclosure agreements should address the requirement to protect confidential information using legally enforceable terms. Confidentiality or non-disclosure agreements are applicable to external party or employees of the organisation. Elements should be selected or added in consideration of the type of the other party and its permissible access or handling of confidential information. To identify requirements for confidentiality or non-disclosure agreements, the following elements should be considered:

i) definition of the information to be protected (e.g. confidential information);

ii) expected duration of an agreement, including cases where confidentiality might need to be maintained indefinitely;

iii) required actions when an agreement is terminated;

iv) responsibilities and actions of signatories to avoid unauthorised information disclosure;

v) ownership of information, trade secrets and intellectual property, and how this relates to the protection of confidential information;

vi) the permitted use of confidential information and rights of the signatory to use information;

vii) the right to audit and monitor activities that involve confidential information;

viii) process for notification and reporting of unauthorised disclosure or confidential information leakage;

ix) terms for information to be returned or destroyed at agreement cessation; and

x) expected actions to be taken in case of a breach of the agreement.

Based on an organisation's information security requirements, other elements may be needed in a confidentiality or non-disclosure agreement.

Confidentiality and non-disclosure agreements should comply with all applicable laws and regulations for the jurisdiction to which they apply.

Requirements for confidentiality and non-disclosure agreements should be reviewed periodically and when changes occur that influence these requirements.

c) Other information

Confidentiality and non-disclosure agreements protect organisational information and inform signatories of their responsibility to protect, use and disclose information in a responsible and authorised manner.

There may be a need for an organisation to use different forms of confidentiality or non-disclosure agreements in different circumstances.

14. System acquisition, development and maintenance

14.1 Security requirements of information systems

To ensure that information security is an integral part of information systems across the entire lifecycle. This also includes the requirements for information systems which provide services over public networks.

14.1.1 Information security requirements analysis and specification

a) Control

The information security related requirements should be included in the requirements for new information systems or enhancements to existing information systems.

b) Implementation guidance

Information security requirements should be identified using various methods such as deriving compliance requirements from policies and regulations, threat modelling, incident reviews, or use of vulnerability thresholds. Results of the ID should be documented and reviewed by all stakeholders.

Information security requirements and controls should reflect the business value of the information involved and the potential negative business impact which might result from lack of adequate security.

ID and management of information security requirements and associated processes should be integrated in early stages of information systems projects. Early consideration of information security requirements, e.g. at the design stage can lead to more effective and cost-efficient solutions.

Information security requirements should also consider:

i) the level of confidence required towards the claimed identity of users, in order to derive user authentication requirements;

ii) access provisioning and authorisation processes, for business users as well as for privileged or technical users;

iii) informing users and operators of their duties and responsibilities;

iv) the required protection needs of the assets involved, in particular regarding availability, confidentiality, integrity;

v) requirements derived from business processes, such as transaction logging and monitoring, non-repudiation requirements; and

vi) requirements mandated by other security controls, e.g. interfaces to logging and monitoring or data leakage detection systems.

For applications that provide services over public networks or which implement transactions, the dedicated clauses 14.1.2 and 14.1.3 should be considered.

If products are acquired, a formal testing and acquisition process should be followed. Contracts with the supplier should address the identified security requirements. Where the security functionality in a proposed product does not satisfy the specified requirement, the risk introduced and associated controls should be reconsidered prior to purchasing the product.

Available guidance for security configuration of the product aligned with the final software/service stack of that system should be evaluated and implemented.

Criteria for accepting products should be defined e.g. in terms of their functionality, which will give assurance that the identified security requirements are met. Products should be evaluated against these criteria before acquisition. Additional functionality should be reviewed to ensure it does not introduce unacceptable additional risks.

c) Other information

ISO/IEC 27005 and ISO 31000 provide guidance on the use of risk management processes to identify controls to meet information security requirements.

14.1.2 Securing application services on public networks

a) Control

Information involved in application services passing over public networks should be protected from fraudulent activity, contract dispute and unauthorised disclosure and modification.

b) Implementation guidance

Information security considerations for application services passing over public networks should include the following:

i) the level of confidence each party requires in each other's claimed identity, e.g. through authentication;

ii) authorisation processes associated with who may approve contents of, issue or sign key transactional documents;

iii) ensuring that communicating partners are fully informed of their authorisations for provision or use of the service;

iv) determining and meeting requirements for confidentiality, integrity, proof of dispatch and receipt of key documents and the non-repudiation of contracts, e.g. associated with tendering and contract processes;

v) the level of trust required in the integrity of key documents;

vi) the protection requirements of any confidential information;

vii) the confidentiality and integrity of any order transactions, payment information, delivery address details and confirmation of receipts;

viii) the degree of verification appropriate to verify payment information supplied by a customer;

ix) selecting the most appropriate settlement form of payment to guard against fraud;

x) the level of protection required to maintain the confidentiality and integrity of order information;

xi) avoidance of loss or duplication of transaction information;

xii) liability associated with any fraudulent transactions; and

xiii) insurance requirements.

Many of the above considerations can be addressed by the application of cryptographic controls (see Clause 10).

Application service arrangements between partners should be supported by a documented agreement which commits both party to the agreed terms of services, including details of authorisation (see Clause 14.1.2 b) ii)).

Resilience requirements against attacks should be considered, which can include requirements for protecting the involved application servers or ensuring the availability of network interconnections required to deliver the service.

c) Other information

Applications accessible via public networks are subject to a range of network related threats, such as fraudulent activities, contract disputes or disclosure of information to the public. Therefore, detailed risk assessments and proper selection of controls are indispensable. Controls required often include cryptographic methods for authentication and securing data transfer.

Application services can make use of secure authentication methods, e.g. using public key cryptography and digital signatures (see Clause 10) to reduce the risks. Also, trusted third party can be used, where such services are needed.

14.1.3 Protecting application services transactions

a) Control

Information involved in application service transactions should be protected to prevent incomplete transmission, misroute, unauthorised message alteration, unauthorised disclosure, unauthorised message duplication or replay.

b) Implementation guidance

Information security considerations for application service transactions should include the following:

i) the use of electronic signatures by each of the party involved in the transaction;

ii) all aspects of the transaction, i.e. ensuring that:

1) user's secret authentication information of all party is valid and verified;

2) the transaction remains confidential; and

3) privacy associated with all party involved is retained.

iii) communications path between all involved party is encrypted;

iv) protocols used to communicate between all involved party are secured;

v) ensuring that the storage of the transaction details is located outside of any publicly accessible environment, e.g. on a storage platform existing on the organisational intranet, and not retained and exposed on a storage medium directly accessible from the Internet; and

vi) where a trusted authority is used (e.g. for the purposes of issuing and maintaining digital signatures or digital certificates) security is integrated and embedded throughout the entire end-to-end certificate/signature management process.

c) Other information

The extent of the controls adopted needs to be adequate with the level of the risk associated with each form of application service transaction.

Transactions may need to comply with legal and regulatory requirements in the jurisdiction which the transaction is generated from, processed via, completed at or stored in.

14.2 Security in development and support processes

To ensure that information security is designed and implemented within the development lifecycle of information systems.

14.2.1 Secure development policy

a) Control

Rules for the development of software and systems should be established and applied to developments within the organisation.

b) Implementation guidance

Secure development is a requirement to build up a secure service, architecture, software and system.

Within a secure development policy, the following aspects should be put under consideration:

i) security of the development environment;

ii) guidance on the security in the software development lifecycle:

1) security in the software development methodology; and

2) secure coding guidelines for each programming language used.

iii) security requirements in the design phase;

iv) security checkpoints within the project milestones;

v) secure repositories;

vi) security in the version control;

vii) required application security knowledge; and

viii) developers' capability of avoiding, finding and fixing vulnerabilities.

Secure programming techniques should be used both for new developments and in code re-use scenarios where the standards applied to development may not be known or were not consistent with current best practices. Secure coding standards should be considered and where relevant mandated for use.

Developers should be trained in their use and testing and code review should verify their use. If development is outsourced, the organisation should obtain assurance that the external party complies with these rules for secure development.

c) Other information

Development may also take place inside applications, e.g. office applications, scripting, browsers and databases.

14.2.2 System change control procedures

a) Control

Changes to systems within the development lifecycle should be controlled by the use of formal change control procedures.

b) Implementation guidance

Formal change control procedures should be documented and enforced to ensure the integrity of system, applications and products, from the early design stages through all subsequent maintenance efforts. Introduction of new systems and major changes to existing systems should follow a formal process of documentation, specification, testing, quality control and managed implementation.

This process should include a risk assessment, analysis of the impacts of changes and specification of security controls needed. This process should also ensure that existing security and control procedures are not compromised, that support programmers are given access only to those parts of the system necessary for their work and that formal agreement and approval for any change is obtained.

Wherever practicable, application and operational change control procedures should be integrated. The change control procedures should include but not be limited to:

i) maintaining a record of agreed authorisation levels;

ii) ensuring changes are submitted by authorised users;

iii) reviewing controls and integrity procedures to ensure that they will not be compromised by the changes;

iv) identifying all software, information, database entities and hardware that require amendment;

v) identifying and checking security critical code to minimise the likelihood of known security weaknesses;

vi) obtaining formal approval for detailed proposals before work commences;

vii) ensuring authorised users accept changes prior to implementation;

viii) ensuring that the system documentation set is updated on the completion of each change and that old documentation is archived or disposed of;

ix) maintaining a version control for all software updates;

x) maintaining an audit trail of all change requests;

xi) ensuring that operating documentation and user procedures are changed as necessary to remain appropriate; and

xii) ensuring that the implementation of changes takes place at the right time and does not disturb the business processes involved.

c) Other information

Changing software can impact the operational environment and vice versa.

Good practice includes the testing of new software in an environment segregated from both the production and development environments. This provides a means of having control over new software and allowing additional protection of operational information that is used for testing purposes. This should include patches, service packs and other updates.

Where automatic updates are considered, the risk to the integrity and availability of the system should be considered against the benefit of speedy deployment of updates. Automatic updates should not be used on critical systems as some updates can cause critical applications to fail.

14.2.3 Technical review of applications after operating platform changes

a) Control

When operating platforms are changed, business critical applications should be reviewed and tested to ensure there is no adverse impact on organisational operations or security.

b) Implementation guidance

This process should cover:

i) review of application control and integrity procedures to ensure that they have not been compromised by the operating platform changes;

ii) ensuring that notification of operating platform changes is provided in time to allow appropriate tests and reviews to take place before implementation; and

iii) ensuring that appropriate changes are made to the BCPs (see Clause 17).

c) Other information

Operating platforms include operating systems, databases and middleware platforms. The control should also be applied for changes of applications.

14.2.4 Restrictions on changes to software packages

a) Control

Modifications to software packages should be discouraged, limited to necessary changes and all changes should be strictly controlled.

b) Implementation guidance

As far as possible and practicable, vendor supplied software packages should be used without modification. Where a software package needs to be modified the following points should be considered:

i) the risk of built-in controls and integrity processes being compromised;

ii) whether the consent of the vendor should be obtained; and

iii) the possibility of obtaining the required changes from the vendor as standard program updates;

iv) the impact if the organisation becomes responsible for the future maintenance of the software as a result of changes; and

v) compatibility with other software in use.

If changes are necessary the original software should be retained and the changes applied to a designated copy. A software update management process should be implemented to ensure the most up to date approved patches and application updates are installed for all authorised software. All changes should be fully tested and documented, so that they can be reapplied, if necessary, to future software upgrades. If required, the modifications should be tested and validated by an independent evaluation body.

14.2.5 Secure system engineering principles

a) Control

Principles for engineering secure systems should be established, documented, maintained and applied to any information system implementation efforts.

b) Implementation guidance

Secure information system engineering procedures based on security engineering principles should be established, documented and applied to in-house information system engineering activities. Security should be designed into all architecture layers (business, data, applications and technology) balancing the need for information security with the need for accessibility. New technology should be analysed for security risks and the design should be reviewed against known attack patterns.

These principles and the established engineering procedures should be regularly reviewed to ensure that they are effectively contributing to enhanced standards of security within the engineering process. They should also be regularly reviewed to ensure that they remain up to date in terms of combating any new potential threats and in remaining applicable to advances in the technologies and solutions being applied.

The established security engineering principles should be applied, where applicable, to outsourced information systems through the contracts and other binding agreements between the organisation and the supplier to whom the organisation outsources. The organisation should confirm that the rigour of suppliers' security engineering principles is comparable with its own.

c) Other information

Application development procedures should apply secure engineering techniques in the development of applications that have input and output interfaces. Secure engineering techniques provide guidance on user authentication techniques, secure session control and data validation, sanitisation and elimination of debugging codes.

14.2.6 Secure development environment

a) Control

Organisations should establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development lifecycle.

b) Implementation guidance

A secure development environment includes people, processes and technology associated with system development and integration.

Organisations should evaluate risks associated with individual system development efforts and establish secure development environments for specific system development efforts, considering:

i) sensitivity of data to be processed, stored and transmitted by the system;

ii) applicable external and internal requirements, e.g. from regulations or policies;

iii) security controls already implemented by the organisation that support system development;

iv) trustworthiness of personnel working in the environment;

v) the degree of outsourcing associated with system development;

vi) the need for segregation between different development environments;

vii) control of access to the development environment;

viii) monitoring of change to the environment and code stored therein;

ix) backups are stored at secure offsite locations; and

x) control over movement of data from and to the environment.

Once the level of protection is determined for a specific development environment, organisations should document corresponding processes in secure development procedures and provide these to all individuals who need them.

14.2.7 Outsourced development

a) Control

The organisation should supervise and monitor the activity of outsourced system development.

b) Implementation guidance

Where system development is outsourced, the following points should be considered across the organisation's entire external supply chain:

i) licensing arrangements, code ownership and intellectual property rights related to the outsourced content;

ii) contractual requirements for secure design, coding and testing practices;

iii) provision of the approved threat model to the external developer;

iv) acceptance testing for the quality and accuracy of the deliverables;

v) provision of evidence that security thresholds were used to establish minimum acceptable levels of security and privacy quality;

vi) provision of evidence that sufficient testing has been applied to guard against the absence of both intentional and unintentional malicious content upon delivery;

vii) provision of evidence that sufficient testing has been applied to guard against the presence of known vulnerabilities;

viii) escrow arrangements, e.g. if source code is no longer available;

ix) contractual right to audit development processes and controls;

x) effective documentation of the build environment used to create deliverables; and

xi) the organisation remains responsible for compliance with applicable laws and control efficiency verification.

c) Other information

Further information on supplier relationships can be found in ISO/IEC 27036.

14.2.8 System security testing

a) Control

Testing of security functionality should be carried out during development.

b) Implementation guidance

New and updated systems require thorough testing and verification during the development processes, including the preparation of a detailed schedule of activities and test inputs and expected outputs under a range of conditions. For in-house developments, such tests should initially be performed by the development team. Independent acceptance testing should then be undertaken (both for in house and for outsourced developments) to ensure that the system works as expected and only as expected. The extent of testing should be in proportion to the importance and nature of the system.

14.2.9 System acceptance testing

a) Control

Acceptance testing programs and related criteria should be established for new information systems, upgrades and new versions.

b) Implementation guidance

System acceptance testing should include testing of information security requirements and adherence to secure system development practices. The testing should also be conducted on received components and integrated systems.

Organisations can leverage automated tools, such as code analysis tools or vulnerability scanners, and should verify the remediation of security related defects.

Testing should be performed in a realistic test environment to ensure that the system will not introduce vulnerabilities to the organisation's environment and that the tests are reliable.

14.3 Test data

To ensure the protection of data used for testing.

14.3.1 Protection of test data

a) Control

Test data should be selected carefully, protected and controlled.

b) Implementation guidance

The use of operational data containing PII or any other confidential information for testing purposes should be avoided. If PII or otherwise confidential information is used for testing purposes, all sensitive details and content should be protected by removal or modification (see ISO/IEC 29101).

The following guidelines should be applied to protect operational data, when used for testing purposes:

i) the access control procedures, which apply to operational application systems, should also apply to test application systems;

ii) there should be separate authorisation each time operational information is copied to a test environment;

iii) operational information should be erased from a test environment immediately after the testing is complete; and

iv) the copying and use of operational information should be logged to provide an audit trail.

c) Other information

System and acceptance testing usually requires substantial volumes of test data that are as close as possible to operational data.

15. Supplier relationships

15.1 Information security in supplier relationships

To ensure protection of the organisation's assets that is accessible by suppliers.

15.1.1 Information security policy for supplier relationships

a) Control

Information security requirements for mitigating the risks associated with supplier's access to the organisation's assets should be agreed with the supplier and documented.

b) Implementation guidance

The organisation should identify and mandate information security controls to specifically address supplier access to the organisation's information in a policy. These controls should address processes and procedures to be implemented by the organisation, as well as those processes and procedures that the organisation should require the supplier to implement, including:

i) identifying and documenting the types of suppliers, e.g. IT services, logistics utilities, financial services, IT infrastructure components, whom the organisation will allow to access its information;

ii) a standardised process and lifecycle for managing supplier relationships;

iii) defining the types of information access that different types of suppliers will be allowed, and monitoring and controlling the access;

iv) minimum information security requirements for each type of information and type of access to serve as the basis for individual supplier agreements based on the organisation's business needs and requirements and its risk profile;

v) processes and procedures for monitoring adherence to established information security requirements for each type of supplier and type of access, including external party review and product validation;

vi) accuracy and completeness controls to ensure the integrity of the information or information processing provided by either party;

vii) types of obligations applicable to suppliers to protect the organisation's information;

viii) handling incidents and contingencies associated with supplier access including responsibilities of both the organisation and suppliers;

ix) resilience and, if necessary, recovery and contingency arrangements to ensure the availability of the information or information processing provided by either party;

x) awareness training for the organisation's personnel involved in acquisitions regarding applicable policies, processes and procedures;

xi) awareness training for the organisation's personnel interacting with supplier personnel regarding appropriate rules of engagement and behaviour based on the type of supplier and the level of supplier access to the organisation's systems and information;

xii) conditions under which information security requirements and controls will be documented in an agreement signed by both party; and

xiii) managing the necessary transitions of information, information processing facilities and anything else that needs to be moved and ensuring that information security is maintained throughout the transition period.

c) Broadcasting-specific implementation guidance

The organisation should identify and mandate information security controls to specifically address supplier access to the organisation's information in a policy.

Broadcasting organisations should require their supplier to perform the following:

i) identifying the supply chain of the supplier involved in handling and/or processing the information;

ii) define the types of information access that different types of suppliers will be allowed, and monitoring and controlling the access;

iii) types of obligations applicable to suppliers to protect the broadcasting organisation's information and condition under which information security requirements and controls should be documented in an agreement signed by both party; and

iv) handling incidents and contingencies associated with supplier access including responsibilities of both the broadcasting organisations and suppliers.

15.1.2 Addressing security within supplier agreement

a) Control

All relevant information security requirements should be established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for, the organisation's information.

b) Implementation guidance

Supplier agreements should be established and documented to ensure that there is no misunderstanding between the organisation and the supplier regarding both party' obligations to fulfil relevant information security requirements.

The following terms should be considered for inclusion in the agreements in order to satisfy the identified information security requirements:

i) description of the information to be provided or accessed and methods of providing or accessing the information;

ii) classification of information according to the organisation's classification scheme; if necessary also mapping between the organisation's own classification scheme and the classification scheme of the supplier;

iii) legal and regulatory requirements, including data protection, intellectual property rights and copyright, and a description of how it will be ensured that they are met;

iv) obligation of each contractual party to implement an agreed set of controls including access control, performance review, monitoring, reporting and auditing;

v) rules of acceptable use of information, including unacceptable use if necessary;

vi) either explicit list of supplier personnel authorised to access or receive the organisation's information or procedures or conditions for authorisation, and removal of the authorisation, for access to or receipt of the organisation's information by supplier personnel;

vii) information security policies relevant to the specific contract;

viii) incident management requirements and procedures (especially notification and collaboration during incident remediation);

ix) training and awareness requirements for specific procedures and information security requirements, e.g. for incident response, authorisation procedures;

x) relevant regulations for sub-contracting, including the controls that need to be implemented;

xi) relevant agreement partners, including a contact person for information security issues;

xii) screening requirements, if any, for supplier's personnel including responsibilities for conducting the screening and notification procedures if screening has not been completed or if the results give cause for doubt or concern;

xiii) right to audit the supplier processes and controls related to the agreement;

xiv) defect resolution and conflict resolution processes;

xv) supplier's obligation to periodically deliver an independent report on the effectiveness of controls and agreement on timely correction of relevant issues raised in the report; and

xvi) supplier's obligations to comply with the organisation's security requirements.

c) Broadcasting-specific implementation guidance

Supplier agreements should be established and documented to ensure that there is no misunderstanding between the broadcasting organisations and the supplier regarding both party' obligations to fulfil relevant information security requirements. The agreements can vary significantly for different services and among the different types of supplier. The agreements should be handle by qualified legal personnel.

15.1.3 Information and communication technology supply chain

a) Control

Agreement with supplier should include requirements to address the information security risks associated with information and communications technology services and product supply chain.

b) Implementation guidance

The following topics should be considered for inclusion in supplier agreements concerning supply chain security:

i) defining information security requirements to apply to information and communication technology product or service acquisition in addition to the general information security requirements for supplier relationships;

ii) for information and communication technology services, requiring that suppliers propagate the organisation's security requirements throughout the supply chain if suppliers subcontract for parts of information and communication technology service provided to the organisation;

iii) for information and communication technology products, requiring that suppliers propagate appropriate security practices throughout the supply chain if these products include components purchased from other suppliers;

iv) implementing a monitoring process and acceptable methods for validating that delivered information and communication technology products and services are adhering to stated security requirements;

v) implementing a process for identifying product or service components that are critical for maintaining functionality and therefore require increased attention and scrutiny when built outside of the organisation especially if the top tier supplier outsources aspects of product or service components to other suppliers;

vi) obtaining assurance that critical components and their origin can be traced throughout the supply chain;

vii) obtaining assurance that the delivered information and communication technology products are functioning as expected without any unexpected or unwanted features;

viii) defining rules for sharing of information regarding the supply chain and any potential issues and compromises among the organisation and suppliers; and

ix) implementing specific processes for managing information and communication technology component lifecycle and availability and associated security risks. This includes managing the risks of components no longer being available due to suppliers no longer being in business or suppliers no longer providing these components due to technology advancements.

c) Broadcasting-specific implementation guidance

Supplier agreements between a broadcasting organisation and its customers should include appropriate controls to ensure the non-disclosure of sensitive customer data. For instance, if directory assistance services are provided by external party, the supplier's agreements should include requirements concerning disclosure of customer data, e.g. their telephone numbers or IDs.

When essential communications together with other communications are provided by suppliers, the broadcasting organisations should ensure existing agreements are fulfilled regarding prioritisation of essential communications throughout the supply chain.

In cases where components provided by the supply chain are integrated into a broadcasting network, the organisation should ensure the integrity and communications functionality of sourced components. Particular attention should be paid to maintenance and "call home" or "trouble reporting" functionalities.

Where services provided by a supplier involve sensitive information, there should be supplier agreements in place. These should include terms prohibiting any sub-contract that allows access to information in scope of the agreement, without prior agreement of the data owner. When it is necessary for a supplier to sub-contract work, broadcasting organisations should ensure that the appropriate levels of protection for that sensitive information have been previously agreed and are maintained throughout the entire supply chain.

15.2 Supplier service delivery management

To maintain an agreed level of information security and service delivery in line with supplier agreements.

15.2.1 Monitoring and review of supplier services

a) Control

Organisations should regularly monitor, review and audit supplier service delivery.

b) Implementation guidance

Monitoring and review of supplier services should ensure that the information security terms and conditions of the agreements are being adhered to and that information security incidents and problems are managed properly.

This should involve a service management relationship process between the organisation and the supplier to:

i) monitor service performance levels to verify adherence to the agreements;

ii) review service reports produced by the supplier and arrange regular progress meetings as required by the agreements;

iii) conduct audits of suppliers, in conjunction with review of independent auditor's reports, if available, and follow-up on issues identified;

iv) provide information about information security incidents and review this information as required by the agreements and any supporting guidelines and procedures;

v) review supplier audit trails and records of information security events, operational problems, failures, tracing of faults and disruptions related to the service delivered;

vi) resolve and manage any identified problems;

vii) review information security aspects of the supplier's relationships with its own suppliers; and

viii) ensure that the supplier maintains sufficient service capability together with workable plans designed to ensure that agreed service continuity levels are maintained following major service failures or disaster (see Clause 17).

The responsibility for managing supplier relationships should be assigned to a designated individual or service management team. In addition, the organisation should ensure that suppliers assign responsibilities for reviewing compliance and enforcing the requirements of the agreements. Sufficient technical skills and resources should be made available to monitor that the requirements of the agreement, in particular the information security requirements, are being met. Appropriate action should be taken when deficiencies in the service delivery are observed.

The organisation should retain sufficient overall control and visibility into all security aspects for sensitive or critical information or information processing facilities accessed, processed or managed by a supplier. The organisation should retain visibility into security activities such as change management, ID of vulnerabilities and information security incident reporting and response through a defined reporting process.

15.2.2 Managing changes to supplier services

a) Control

Changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures and controls, should be managed, taking account of the criticality of business information, systems and processes involved and re-assessment of risks.

b) Implementation guidance

The following aspects should be taken into consideration:

i) changes to supplier agreements;

ii) changes made by the organisation to implement:

1) enhancements to the current services offered;

2) development of any new applications and systems;

3) modifications or updates of the organisation's policies and procedures; and

4) new or changed controls to resolve information security incidents and to improve security.

iii) changes in supplier services to implement:

1) changes and enhancement to networks;

2) use of new technologies;

3) adoption of new products or newer versions/releases;

4) new development tools and environments;

5) changes to physical location of service facilities;

6) change of suppliers; and

7) sub-contracting to another supplier.

16. Information security incident management

16.1 Management of information security incidents and improvements

To ensure a consistent and effective approach to the management of information security incidents, including communication in security events and weaknesses.

16.1.1 Responsibilities and procedures

a) Control

Management responsibilities and procedures should be established to ensure a quick, effective and orderly response to information security incidents.

b) Implementation guidance

The following guidelines for management responsibilities and procedures with regard to information security incident management should be considered:

i) management responsibilities should be established to ensure that the following procedures are developed and communicated adequately within the organisation:

1) procedures for incident response planning and preparation;

2) procedures for monitoring, detecting, analysing and reporting of information security events and incidents;

3) procedures for logging incident management activities;

4) procedures for handling of forensic evidence;

5) procedures for assessment of and decision on information security events and assessment of information security weaknesses; and

6) procedures for response including those for escalation, controlled recovery from an incident and communication to internal and external people or organisations.

ii) procedures established should ensure that:

1) competent personnel handle the issues related to information security incidents within the organisation;

2) a point of contact for security incidents' detection and reporting is implemented; and

3) appropriate contacts with authorities, external interest groups or forums that handle the issues related to information security incidents are maintained.

iii) reporting procedures should include:

1) preparing information security event reporting forms to support the reporting action and to help the person reporting to remember all necessary actions in case of an information security event;

2) the procedure to be undertaken in case of an information security event, e.g. noting all details immediately, such as type of non-compliance or breach, occurring malfunction, messages on the screen and immediately reporting to the point of contact and taking only coordinated actions;
3) reference to an established formal disciplinary process for dealing with employees who commit security breaches; and

4) suitable feedback processes to ensure that those persons reporting information security events are notified of results after the issue has been dealt with and closed.

The objectives for information security incident management should be agreed with management, and it should be ensured that those responsible for information security incident management understand the organisation's priorities for handling information security incidents.

16.1.2 Reporting information security events

a) Control

Information security events should be reported through appropriate management channels as quickly as possible.

b) Implementation guidance

All employees and contractors should be made aware of their responsibility to report information security events as quickly as possible. They should also be aware of the procedure for reporting information security events and the point of contact to which the events should be reported.

Situations to be considered for information security event reporting include:

i) ineffective security control;

ii) breach of information integrity, confidentiality or availability expectations;

iii) human errors;

iv) non-compliances with policies or guidelines;

v) breaches of physical security arrangements;

vi) uncontrolled system changes;

vii) malfunctions of software or hardware; and

viii) access violations.

c) Other information

Malfunctions or other anomalous system behaviour may be an indicator of a security attack or actual security breach and should therefore always be reported as an information security event.

16.1.3 Reporting security weaknesses

a) Control

Employees and contractors using the organisation's information systems and services should be required to note and report any observed or suspected information security weaknesses in systems or services.

b) Implementation guidance

All employees and contractors should report these matters to the point of contact as quickly as possible in order to prevent information security incidents. The reporting mechanism should be as easy, accessible and available as possible.

c) Other information

Employees and contractors should be advised not to attempt to prove suspected security weaknesses.

Testing weaknesses might be interpreted as a potential misuse of the system and could also cause damage to the information system or service and result in legal liability for the individual performing the testing.

16.1.4 Assessment of and decision on information security events

a) Control

Information security events should be assessed and it should be decided if they are to be classified as information security incidents.

b) Implementation guidance

The point of contact should assess each information security event using the agreed information security event and incident classification scale and decide whether the event should be classified as an information security incident. Classification and prioritisation of incidents can help to identify the impact and extent of an incident.

In cases where the organisation has an Information Security Incident Response Team (ISIRT), the assessment and decision can be forwarded to the ISIRT for confirmation or reassessment.
Results of the assessment and decision should be recorded in detail for the purpose of future reference and verification.

c) Other information

All relevant party including employees, external party users and contractors should be made aware of such classification.

16.1.5 Response to information security incidents

a) Control

Information security incidents should be responded to in accordance with the documented procedures.

b) Implementation guidance

Information security incidents should be responded to by a nominated point of contact and other relevant persons of the organisation or external party.

The response should include the following:

i) collecting evidence as soon as possible after the occurrence;

ii) conducting information security forensics analysis, as required;

iii) escalation, as required;

iv) ensuring that all involved response activities are properly logged for later analysis;

v) communicating the existence of the information security incident or any relevant details thereof to other internal and external people or organisations with a need-to-know;

vi) dealing with information security weakness(es) found to cause or contribute to the incident; and

vii) once the incident has been successfully dealt with, formally closing and recording it.

Post-incident analysis should take place, as necessary, to identify the source of the incident.

16.1.6 Learning from information security incidents

a) Control

Knowledge gained from analysing and resolving information security incidents should be used to reduce the likelihood or impact of future incidents.

b) Implementation guidance

There should be mechanisms in place to enable the types, volumes and costs of information security incidents to be quantified and monitored. The information gained from the evaluation of information security incidents should be used to identify recurring or high impact incidents.

c) Broadcasting-specific implementation guidance

Broadcasting organisations should establish mechanisms and/or procedures for sharing the lessons learnt and improving the incident management, taking account of the following actions:

i) hold a post-incident meeting, which includes on the agenda the lessons learned - this meeting should consider ways for improving security measures and the incident handling process itself;

ii) collect incident data, such as number of incidents handled, total hours on involvement and costs, and use it for improvement of the incident management scheme; and

iii) retain related evidence in consideration of prosecution, law/regulation and cost (see 17.1.7).

16.1.7 Collection of evidence

a) Control

The organisation should define and apply procedures for the ID, collection, acquisition and preservation of information, which can serve as evidence.

b) Implementation guidance

Internal procedures should be developed and followed when dealing with evidence for the purposes of disciplinary and legal action.

In general, these procedures for evidence should provide processes of ID, collection, acquisition and preservation of evidence in accordance with different types of media, devices and status of devices, e.g. powered on or off. The procedures should take account of:

i) chain of custody;

ii) safety of evidence;

iii) safety of personnel;

iv) roles and responsibilities of personnel involved;

v) competency of personnel;

vi) documentation; and

vii) briefing.

Where available, certification or other relevant means of qualification of personnel and tools should be sought, so as to strengthen the value of the preserved evidence.

Forensic evidence may transcend organisational or jurisdictional boundaries. In such cases, it should be ensured that the organisation is entitled to collect the required information as forensic evidence. The requirements of different jurisdictions should also be considered to maximise chances of admission across the relevant jurisdictions.

c) Other information

ID is the process involving the search for, recognition and documentation of potential evidence. Collection is the process of gathering the physical items that can contain potential evidence.

Acquisition is the process of creating a copy of data within a defined set. Preservation is the process to maintain and safeguard the integrity and original condition of the potential evidence.

When an information security event is first detected, it may not be obvious whether or not the event will result in court action. Therefore, the danger exists that necessary evidence is destroyed intentionally or

accidentally before the seriousness of the incident is realised. It is advisable to involve a lawyer or the police early in any contemplated legal action and take advice on the evidence required.

ISO/IEC 27037 provides guidelines for ID, collection, acquisition and preservation of digital evidence.

17. Information security aspects of Business Continuity Management (BCM)

17.1 Information security continuity

Information security continuity should be embedded in the organisation's BCM systems.

17.1.1 Planning information security continuity

a) Control

The organisation should determine its requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or disaster.

b) Implementation guidance

An organisation should determine whether the continuity of information security is captured within the BCM process or within the disaster recovery management process. Information security requirements should be determined when planning for business continuity and disaster recovery.

In the absence of formal business continuity and disaster recovery planning, information security management should assume that information security requirements remain the same in adverse situations, compared to normal operational conditions. Alternatively, an organisation could perform a business impact analysis for information security aspects to determine the information security requirements applicable to adverse situations.

c) Other information

In order to reduce the time and effort of an ‘additional’ business impact analysis for information security, it is recommended to capture information security aspects within the normal BCM or disaster recovery management business impact analysis. This implies that the information security continuity requirements are explicitly formulated in the BCM or disaster recovery management processes.

Information on BCM can be found in ISO/IEC 27031, ISO 22313 and ISO 22301.

17.1.2 Implementing information security continuity

a) Control

The organisation should establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation.

b) Implementation guidance

An organisation should ensure that:

i) an adequate management structure is in place to prepare for, mitigate and respond to a disruptive event using personnel with the necessary authority, experience and competence;

ii) incident response personnel with the necessary responsibility, authority and competence to manage an incident and maintain information security are nominated; and

iii) documented plans, response and recovery procedures are developed and approved, detailing how the organisation will manage a disruptive event and will maintain its information security to a predetermined level, based on management-approved information security continuity objectives.

According to the information security continuity requirements, the organisation should establish, document, implement and maintain:

i) information security controls within business continuity or disaster recovery processes, procedures and supporting systems and tools;

ii) processes, procedures and implementation changes to maintain existing information security controls during an adverse situation; and

iii) compensating controls for information security controls that cannot be maintained during an adverse situation.

c) Broadcasting-specific implementation guidance

Plan for graceful degradation of service with priority given to emergency services and the least critical services being degraded or stopped in priority order.

The BCP should contain provision for information security continuity to protect information in various forms. In developing and implementing the BCP, broadcasting organisations should consider the inclusion of a disaster recovery plan for broadcasting services and ensuring essential communications of broadcasting service customers.

Broadcasting organisations should also consider when to dispatch their staff to broadcasting operating areas for disaster recovery.

17.1.3 Verifying, review and evaluate information security continuity

a) Control

The organisation should verify the established and implement information security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations.

b) Implementation guidance

Organisational, technical, procedural and process changes, whether in an operational or continuity context, can lead to changes in information security continuity requirements. In such cases, the continuity of processes, procedures and controls for information security should be reviewed against these changed requirements.

Organisations should verify their information security management continuity by:

i) exercising and testing the functionality of information security continuity processes, procedures and controls to ensure that they are consistent with the information security continuity objectives;

ii) exercising and testing the knowledge and routine to operate information security continuity processes, procedures and controls to ensure that their performance is consistent with the information security continuity objectives; and

iii) reviewing the validity and effectiveness of information security continuity measures when information systems, information security processes, procedures and controls or BCM/disaster recovery management processes and solutions change.

17.2 Redundancies

To ensure availability of information processing facilities.

17.2.1 Availability of information processing facilities

a) Control

Information processing facilities should be implemented with redundancy sufficient to meet availability requirements.

b) Implementation guidance

Organisations should identify business requirements for the availability of information systems. Where the availability cannot be guaranteed using the existing systems architecture, redundant components or architectures should be considered.
Where applicable, redundant information systems should be tested to ensure the failover from one component to another component works as intended.

c) Broadcasting-specific implementation guidance

Where the availability cannot be guaranteed using the existing system architecture, redundant components or architectures should be considered, e.g. redundant power supply, switching fabric, network, interface, databases in active-active or active-passive setup.
The implementation redundancies can introduce risks to the integrity or confidentiality of information and information systems, which need to be considered when designing information system.

18. Compliance

18.1 Compliance with legal and contractual requirements

To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements.

18.1.1 Identification of applicable legislation and contractual requirements

a) Control

All relevant legislative statutory, regulatory, contractual requirements and the organisation's approach to meet these requirements should be explicitly identified, documented and kept up to date for each information system and the organisation.

b) Implementation guidance

The specific controls and individual responsibilities to meet these requirements should also be defined and documented.

Managers should identify all legislation applicable to their organisation in order to meet the requirements for their type of business. If the organisation conducts business in other countries, managers should consider compliance in all relevant countries.

18.1.2 Intellectual property rights

a) Control

Appropriate procedures should be implemented to ensure compliance with legislative, regulatory and contractual requirements related to intellectual property rights and use of proprietary software products.

b) Implementation guidance

The following guidelines should be considered to protect any material that may be considered intellectual property:

i) publishing an intellectual property rights compliance policy which defines the legal use of software and information products;

ii) acquiring software only through known and reputable sources, to ensure that copyright is not violated;

iii) maintaining awareness of policies to protect intellectual property rights and giving notice of the intent to take disciplinary action against personnel breaching them;

iv) maintaining appropriate asset registers and identifying all assets with requirements to protect intellectual property rights;

v) maintaining proof and evidence of ownership of licences, master disks, manuals, etc.;

vi) implementing controls to ensure that any maximum number of users permitted within the licence is not exceeded;

vii) carrying out reviews that only authorised software and licensed products are installed;

viii) providing a policy for maintaining appropriate licence conditions;

ix) providing a policy for disposing of or transferring software to others;

x) complying with terms and conditions for software and information obtained from public networks;

xi) not duplicating, converting to another format or extracting from commercial recordings (film, audio) other than permitted by copyright law; and

xii) not copying in full or in part, books, articles, reports or other documents, other than permitted by copyright law.

c) Other information

Intellectual property rights include software or document copyright, design rights, trademarks, patents and source code licences.

Proprietary software products are usually supplied under a licence agreement that specifies licence terms and conditions, for example, limiting the use of the products to specified machines or limiting copying to the creation of backup copies only. The importance and awareness of intellectual property rights should be communicated to staff for software developed by the organisation.

Legislative, regulatory and contractual requirements may place restrictions on the copying of proprietary material. In particular, they may require that only material that is developed by the organisation or that is licensed or provided by the developer to the organisation, can be used. Copyright infringement can lead to legal action, which may involve fines and criminal proceedings.

18.1.3 Protection of records

a) Control

Records should be protected from loss, destruction, falsification, unauthorised access and unauthorised release, in accordance with legislative, regulatory, contractual and business requirements.

b) Implementation guidance

When deciding upon protection of specific organisational records, their corresponding classification based on the organisation's classification scheme, should be considered. Records should be categorised into record types, e.g. accounting records, database records, transaction logs, audit logs and operational procedures, each with details of retention periods and type of allowable storage media, e.g. paper, microfiche, magnetic, optical. Any related cryptographic keys and programs associated with encrypted archives or digital signatures, should also be stored to enable decryption of the records for the length of time the records are retained.

Consideration should be given to the possibility of deterioration of media used for storage of records. Storage and handling procedures should be implemented in accordance with manufacturer's recommendations.

Where electronic storage media are chosen, procedures to ensure the ability to access data (both media and format readability) throughout the retention period should be established to safeguard against loss due to future technology change.

Data storage systems should be chosen such that required data can be retrieved in an acceptable timeframe and format, depending on the requirements to be fulfilled.

The system of storage and handling should ensure ID of records and of their retention period as defined by national or regional legislation or regulations, if applicable. This system should permit appropriate destruction of records after that period if they are not needed by the organisation.
To meet these record safeguarding objectives, the following steps should be taken within an organisation:

i) guidelines should be issued on the retention, storage, handling and disposal of records and information;

ii) a retention schedule should be drawn up identifying records and the period of time for which they should be retained; and

iii) an inventory of sources of key information should be maintained.

c) Other information

Some records may need to be securely retained to meet statutory, regulatory or contractual requirements, as well as to support essential business activities. Examples include records that may be required as evidence that an organisation operates within statutory or regulatory rules, to ensure defence against potential civil or criminal action or to confirm the financial status of an organisation to shareholders, external party and auditors. National law or regulation may set the time period and data content for information retention.

Further information about managing organisational records can be found in ISO 15489-1.

18.1.4 Privacy and protection of personally identifiable information

a) Control

Privacy and protection of PII should be ensured as required in relevant legislation and regulation where applicable.

b) Implementation guidance

An organisation's data policy for privacy and protection of PII should be developed and implemented. This policy should be communicated to all persons involved in the processing of PII.

Compliance with this policy and all relevant legislation and regulations concerning the protection of the privacy of people and the protection of PII requires appropriate management structure and control. Often this is best achieved by the appointment of a person responsible, such as a privacy officer, who should provide guidance to managers, users and service providers on their individual responsibilities and the specific procedures that should be followed. Responsibility for handling PII and ensuring awareness of the privacy principles should be dealt with in accordance with relevant legislation and regulations. Appropriate technical and organisational measures to protect PII should be implemented.

c) Other information

ISO/IEC 29100 provides a high-level framework for the PII information within information and communication technology systems. A number of countries have introduced legislation placing controls on the collection, processing and transmission of PII (generally information on living individuals who can be identified from that information). Depending on the respective national legislation, such controls may impose duties on those collecting, processing and disseminating PII, and may also restrict the ability to transfer PII to other countries.

18.1.5 Regulation of cryptographic controls

a) Control

Cryptographic controls should be used in compliance with all relevant agreements, legislation and regulations.

b) Implementation guidance

The following items should be considered for compliance with the relevant agreements, laws and regulations:

i) restrictions on import or export of computer hardware and software for performing cryptographic functions;

ii) restrictions on import or export of computer hardware and software which is designed to have cryptographic functions added to it;

iii) restrictions on the usage of encryption; and

iv) mandatory or discretionary methods of access by the countries' authorities to information encrypted by hardware or software to provide confidentiality of content.

Legal advice should be sought to ensure compliance with relevant legislation and regulations. Before encrypted information or cryptographic controls are moved across jurisdictional borders, legal advice should also be taken.

18.2 Information security reviews

To ensure that information security is implemented and operated in accordance with the organisational policies and procedures.

18.2.1 Independent review of information security

a) Control

The organisation's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes and procedures for information security) should be reviewed independently at planned intervals or when significant changes occur.

b) Implementation guidance

Management should initiate the independent review. Such an independent review is necessary to ensure the continuing suitability, adequacy and effectiveness of the organisation's approach to managing information security. The review should include assessing opportunities for improvement and the need for changes to the approach to security, including the policy and control objectives.

Such a review should be carried out by individuals independent of the area under review, i.e. the internal audit function, an independent manager or an external party organisation specialising in such reviews. Individuals carrying out these reviews should have the appropriate skills and experience.

The results of the independent review should be recorded and reported to the management who initiated the review. These records should be maintained.

If the independent review identifies that the organisation's approach and implementation to managing information security is inadequate, e.g. documented objectives and requirements are not met or not compliant with the direction for information security stated in the information security policies, management should consider corrective actions.

c) Other information

ISO/IEC 27007 and ISO/IEC TR 27008 also provide guidance for carrying out the independent review.

18.2.2 Compliance with security policies and standards

a) Control

Managers should regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security requirements.

b) Implementation guidance

Managers should identify how to review that information security requirements defined in policies, standards and other applicable regulations are met. Automatic measurement and reporting tools should be considered for efficient regular review.

If any non-compliance is found as a result of the review, managers should:

i) identify the causes of the non-compliance;

ii) evaluate the need for actions to achieve compliance;

iii) implement appropriate corrective action; and

iv) review the corrective action taken to verify its effectiveness and identify any deficiencies or weaknesses.

Results of reviews and corrective actions carried out by managers should be recorded and these records should be maintained. Managers should report the results to the persons carrying out independent reviews when an independent review takes place in the area of their responsibility.

c) Other information

Operational monitoring of system use is covered in Clause 12.4.

18.2.3 Technical compliance review

a) Control

Information systems should be regularly reviewed for compliance with the organisation's information security policies and standards.

b) Implementation guidance

Technical compliance should be reviewed preferably with the assistance of automated tools, which generate technical reports for subsequent interpretation by a technical specialist. Alternatively, manual reviews (supported by appropriate software tools, if necessary) by an experienced system engineer could be performed.

If penetration tests or vulnerability assessments are used, caution should be exercised as such activities could lead to a compromise of the security of the system. Such tests should be planned, documented and repeatable.

Any technical compliance review should only be carried out by competent, authorised persons or under the supervision of such persons.

c) Other information

Technical compliance reviews involve the examination of operational systems to ensure that hardware and software controls have been correctly implemented. This type of compliance review requires specialist technical expertise.

Compliance reviews also cover, for example, penetration testing and vulnerability assessments, which might carry out by independent experts specifically contracted for this purpose. This can be useful in detecting vulnerabilities in the system and for inspecting how effective the controls are in preventing unauthorised access due to this vulnerability.

Penetration testing and vulnerability assessments provide a snapshot of a system in a specific state at a specific time. The snapshot limited to those portions of the system actually tested during the penetration attempts. Penetration testing and vulnerability assessments are not a substitute for risk assessment.

ISO/IEC TR 27008 provides specific guidance regarding technical compliance reviews.

d) Broadcasting-specific implementation guidance

Broadcasting organisations should identify all legislation applicable to their organisation in relation to information security in order to meet the requirements for their type of business with the assistance from legal professional.

Table 2 shows the examples of legislative statutory, regulatory, contractual agreements.

Table 2. Examples of legislative statutory, regulatory and contractual agreements

Act	Example of requirement related to information security
Company Act 1965 An Act relating to companies.	Account and Audit - Section 167 "Every company and its directors must present an audited profit and loss account and balance sheet together with a directors' report, signed by the directors, with regard to the state of affairs of the company at the Annual General Meeting (AGM). The period for such presentation to the AGM IS, Within or 18 months after incorporation of a company, and Every 5 months and once at least in every calendar year."
Personal Data Protection Act 2010 An Act to regulate the processing of personal data in commercial transactions and to provide for matters connected therewith and incidental thereto.	Section 9. Security Principle "A data user shall, when processing personal data, take practical steps to protect the personal data from any loss, misuse, modification, unauthorised or accidental access or disclosure, alteration or destruction."
Malaysian Communications and Multimedia Commission Act 1998 An act to provide for the establishment of the Malaysian Communications and multimedia Commission with powers to supervise and regulate the communications and multimedia activities in Malaysia, and to enforce the communications and multimedia laws of Malaysia, and for related matters.	Obligation of secrecy "52. (1) (a) no member of the Commission or any of its committees or any employee or agent of the Commission or any person attending any meeting of the Commission or any of its committees, whether during his tenure of office or during his employment or thereafter, shall disclose any information obtained by him in the course of his duties; and (b) no other person who has by any means access to any information or document relating to the affairs of the Commission shall disclose such information or document."
Communications and Multimedia Act 1998 An act to provide for and to regulate the converging communications and multimedia industries, and for incidental matters.	Provision of information "73. (4) Any person required to provide information under subsection (2) shall ensure that the information provided is true, accurate and complete and such person shall provide a representation to that effect, including a representation that he is not aware of any other information which would make the information provided untrue or misleading."
The Malaysian Communications and Multimedia Content Code Statutory duty sets out the guidelines and procedures for good practice and standards of content disseminated to audiences by service providers in the communications and multimedia industry in Malaysia.	2.0 General Principles 2.3 The principle of ensuring that Content shall not be indecent, obscene, false, menacing or offensive shall be observed. 7.0 False Content 7.1 Content, which contains false material and is likely to mislead, due amongst others to incomplete information is to be avoided. Content providers must observe measures outlined in specific parts of this Code to limit the likelihood of perpetuating untruths via the communication of false content.

Table 2. Examples of legislative statutory, regulatory and contractual agreements *(continued)*

Act	Example of requirement related to information security
Digital Signature Act 1997 An Act to make provision for, and to regulate the use of, digital signatures and to provide for matters connected there with.	Functions of licensed certification authorities "6. (2) The licensed certification authority shall, before issuing any certificate under this Act, take all reasonable measures to check for proper identification of the subscriber to be listed in the certificate."
Computer Crimes Act 1997 An Act to provide for offences relating to the misuse of computers.	Unauthorised access to computer material "3. (1) A person shall be guilty of an offence if: (a) he causes a computer to perform any function with intent to secure access to any program or data held in any computer; (b) the access he intends to secure is unauthorised; and (c) he knows at the time when he causes the computer to perform the function that is the case."
Defamation Act 1957 An Act relating to the law of libel and slander and other malicious falsehoods.	Reports of judicial proceedings "11. (1) A fair and accurate and contemporaneous report of proceedings publicly heard before any court lawfully exercising judicial authority within Malaysia and of the judgment, sentence or finding of any such court shall be absolutely privileged, and any fair and bona fide comment thereon shall be protected, although such judgment, sentence or finding be subsequently reversed, quashed or varied, unless at the time of the publication of such report or comment the defendant who claims the protection afforded by this section knew or ought to have known of such reversal, quashing or variation. (2) Nothing in this section shall authorise the publication of any blasphemous, seditious or indecent matter or any matter the publication of which is prohibited by law."
Electronic Commerce Act 2006 An Act to provide for legal recognition of electronic messages in commercial transactions, the use of the electronic messages to fulfil legal requirements and to enable and facilitate commercial transactions through the use of electronic means and other matters connected therewith.	Signature "9. (1) Where any law requires a signature of a person on a document, the requirement of the law is fulfilled, if the document is in the form of an electronic message, by an electronic signature Which: (a) is attached to or is logically associated with the electronic message; (b) adequately identifies the person and adequately indicates the person's approval of the information to which the signature relates; and (c) is as reliable as is appropriate given the purpose for which, and the circumstances in which, the signature is required."

Table 2. Examples of legislative statutory, regulatory and contractual agreements *(concluded)*

Act	Example of requirement related to information security
Subscriber Agreement	Agreements establish by broadcasting organisations with their subscriber.
Copyright Act 1987 An Act to make better provisions in the law relating to copyright and for other matters connected therewith.	Access to computerised or digitalised data "45A. (1) Any Assistant Controller or a police officer not below the rank of Inspector shall, in the exercise of his powers under section 44, if it is necessary, be given access to computerised or digitalised data whether stored in a computer or any other medium. (2) For the purpose of this section, access includes being provided with the necessary password, encryption code, decryption code, software or hardware and any other means required to enable comprehension of the computerised data."

Annex A
(normative)

Normative reference

Communications and Multimedia Act 1998

ISO 15489-1, *Information and documentation - Records management - Part 1: Concepts and principles*

ISO 22301, *Societal security - Business continuity management systems - Requirements*

ISO 22313, *Societal security - Business continuity management systems - Guidance*

ISO 31000, *Risk management - Principles and guideline*

ISO/IEC 11770, *Information technology - Security techniques - Key management*

ISO/IEC 27005, *Information Security risk management*

ISO/IEC 27007, *Guidelines for information security management systems auditing*

ISO/IEC 27011, *Information technology - Security techniques - Code of practice for information security controls based on ISO/IEC 27002 for telecommunications organisations*

ISO/IEC 27031, *Guidelines for information and communication technology readiness for business continuity*

ISO/IEC 27033, *Information technology - Security techniques - Network security - Part 1: Overview and concepts*

ISO/IEC 27036, *Information security for supplier relationships - Part 1: Overview and concepts*

ISO/IEC 27037, *Guidelines for identification, collection, acquisition and preservation of digital evidence*

ISO/IEC 29100, *Information technology - Security techniques - Privacy framework*

ISO/IEC 29101, *Information technology - Security techniques - Privacy architecture framework*

ISO/IEC TR 27008, *Information technology - Security techniques - Guidelines for auditors on information security controls*

ITU-T X.1051, *Information technology - Security techniques - Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organizations*

Bibliography

[1] MCMC Network Security Centre Standard Operating Procedure

[2] MCMC MTSFB TC G009, *Requirements for Information and Network Security*

[3] ISO/IEC 11770-2, *Information technology - Security techniques - Key management - Part 2: Mechanisms using symmetric techniques*

[4] ISO/IEC 11770-3, *Information technology - Security techniques - Key management - Part 3: Mechanisms using symmetric techniques*

[5] ISO/IEC 11770-4, *Information technology - Security techniques - Key management - Part 4: Mechanism based on weak secrets*

[6] ISO/IEC 27000, *Information technology - Security techniques - Information security management systems - Overview and vocabulary*

[7] ISO/IEC 27001, *Information technology - Security techniques - Information security management systems - Requirements*

[8] ISO/IEC 27002, *Information technology - Security techniques - Code of practice for information security controls*

Acknowledgements

Members of the Information and Network Security Sub Working Group (INS SWG)

Ms Rafeah Omar (Chairman)	Telekom Malaysia Berhad
Ms Nur Shahidah Senin (Secretariat)	Malaysian Technical Standards Forum Bhd
Mr Mohammad Hafizal Mohammed Ariffin/ Mr Ahmad Tarmimi Che Abdul Aziz	Al Hijrah Media Corporation
Mr Kheirul Hisyam Mohamed/ Mr Muhammad Fithri Zainal	Altel Communications Sdn Bhd
Mr Mohamad Isa Mohd Razhali	MEASAT Broadcast Network Sdn Bhd
Mr Mohd Said Sarami/ Mr Mohd Fazrul Azha Saidal Hadzri	MYTV Broadcasting Sdn Bhd
Mr Thaib Mustafa	Telekom Applied Business Sdn Bhd
Mr Ahmad Zikri Ahmad Sofi	Telekom Malaysia Berhad
Dr Amna Saad	Universiti Kuala Lumpur