Offis Pty Ltd ABN 70 077 283 811
55 Pyrmont Bridge Road
Pyrmont NSW 2009 Australia

P 1300 977 623
F +61 2 8001 1145
W www.offis.com.au

Offis
MULTI-CLOUD SERVICES

Offis Pty Ltd

Information Security Policy

Version 10.3

The Information Security Program for Offis consists of a series of documents, including this document on the organisation’s Information Security Policy. The high-level policy statements contained in this document are based on business requirements and security principles. The policy statements provide general mandatory security requirements and instructions supported by Offis Executive Management.

Version Control

Version	Date	Comments	Author
10.0	13/4/2017	New revision	David Hoh
10.1	20/5/2017	Approved by Franck	Franck Demoiseau
10.2	3/5/2018	Updated document header	David Hoh
10.3	25/3/2019	Updated document classification	David Hoh

This document has been prepared by Offis and is only intended for the review of the individual or entity named above. This document contains information that is confidential and privileged. You are hereby notified that any dissemination, distribution or copying of this document is strictly prohibited without the written consent of Offis. If you have received this documentation in error, please notify us immediately by return email or telephone +61 2 9776 2300 and destroy this document.

Offis follow principles, guidelines and standards issued by but not limited to the following originations; ITIL, NIST, PCI, CIRT, AS/NZS ISO/IEC 27001 and 27002 and the Australian Government. Policy statement categories follow the ISO/IEC 27002:2013 code of practice.

Table of Contents

1. Introduction

Offis is committed to protecting the confidentiality, integrity and availability of all physical and electronic information that is processed, stored and transmitted by information systems belonging to the organisation and its customers. The nature of the organisation's business demands that information security is handled with the utmost importance, and the Information Security Policy recognises the commitment and diligence required by all relevant parties to achieve this.

1.1 Purpose

The purpose of this policy is to establish the level of system and data confidentiality, integrity and availability used across all functions of the organisation's business. It provides an outline of the security principles and policy statements by which all Offis employees and users must abide by.

Effective implementation of this policy will minimise the likelihood of confidential and proprietary information and technology being disclosed to unauthorised parties.

1.2 Scope

The Information Security Policy applies to all business units of the organisation as a general policy. However, there will be sections of the policy which are not applicable to all areas of the business.

Both internal and customer environments within the organisation's core business function are included in the scope of the policy.

2. Information Security

2.1 Mission Statement

Offis and Offis employees have an inherent responsibility to protect the physical information assets of the company as well as confidential member data and intellectual capital owned by the company. These critical assets must be safeguarded to mitigate any potential impacts to Offis and Offis' members. Information security is, therefore, a critical business function that should be incorporated into all aspects of Offis' business practices and operations.

To achieve this objective, policies, standards, guidelines, and procedures have been created to ensure secure business practices are in place at Offis. Information security is a foundational business practice that must be incorporated into planning, development, operations, administration, sales and marketing, as each of these business functions requires specific safeguards to be in place to mitigate the risk associated with normal business activities.

Offis is subject to numerous State and Federal Information Security and Privacy laws and regulations, which if not complied with, could potentially result in fines, audits, loss of employee and customer confidence, and direct financial impact to the company. Compliance with all applicable regulations is the responsibility of every employee at Offis.

All Offis employees are responsible for familiarising themselves with and complying with all Offis policies, procedures and standards dealing with security.

2.2 Definition

The US Code Title 44, Chapter 35, Subchapter III, § 3542 defines Information Security as follows:

(1) The term "information security" means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide -

> *(A) integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity;*
>
> *(B) confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and*
>
> *(C) availability, which means ensuring timely and reliable access to and use of information.*

The policies in this document support these objectives.

2.3 Importance of Security

Offis requires information security to protect information assets from security threats. It is critical to protect the system environment to maintain a competitive advantage in the marketplace, to ensure profitability, and to secure and maintain member and partner trust and confidence.

Security threats originate at a wide variety of sources, including computer-assisted fraud, industrial espionage, sabotage, vandalism and natural disasters. Computer viruses, unethical hacking and denial of service attacks are examples of threats encountered while operating over the Internet. These types of threats are becoming increasingly more common, more ambitious and more sophisticated.

2.4 Protection Philosophy

Offis' protection philosophy provides the intent and direction behind our protection policies, procedures, and control. This philosophy is comprised of three tenets:

1. **Security is everyone's responsibility.** Maintaining an effective and efficient security posture for Offis requires a proactive stance on security issues from everyone. Security is not "somebody else's problem"; as a member of Offis, you have the responsibility to adhere to the security policies and procedures of the company and to take issue with those who are not doing the same.

2. **Security permeates the Offis organisation.** Security is not just focused on physical and technical "border control." Rather, Offis seeks to ensure reasonable and appropriate levels of security awareness and protection throughout our organisation and infrastructure. There is no place in our business where security is not a consideration.

3. **Security is a business enabler.** A strong security foundation, proactively enabled and maintained, becomes an effective market differentiator for our company. Security has a direct impact on our viability within the marketplace, and must be treated as a valued commodity.

The tenets of our philosophy of protection are mutually supportive; ignoring any one tenet in favour of another undermines the overall security posture of our organisation.

2.5 Critical Success Factors

The following factors are critical to the successful implementation of security within Offis:

- Comprehensive security policies, objectives and initiatives that clearly reflect Offis' business objectives
- A security approach that is consistent with Offis' culture
- Highly visible support from Offis' management
- Solid understanding of security requirements and risk management practices
- Effective communication of security to all Offis managers, associates, partners, clients, vendors and developers
- Guidance on information security policy to all Offis managers, associates, partners, clients, vendors and developers
- Information security awareness and training
- Continual review and measurement of the effectiveness and efficiency of security controls and mechanisms
- Timely adjustments to the security posture by addressing deficiencies and by reflecting changes in Offis' business objectives as necessary
- Annual review of the information security policy to update policy as needed to reflect changes to business objectives or the risk environment

2.6 Program Structure

Offis' Information Security Program is structured in such a way to give flexibility as required by the business objectives and needs while maintaining consistency across the company. Frequently, the weakest link is the link that breaks the security chain and causes a breach in security. Through consistent application of Information Security across the company, any weak areas are compensated for and the organisation is stronger overall.

The Information Security Program follows this tiered structure:

- Information Security Policy
- Information Security Standards and Guidelines
- Information Security Specific Configurations and Procedures

The hierarchy lends support as you progress up the tiers and becomes more detailed as you progress down the tiers. In this way, all actions taken have a basis in policy and directly support the policy or policies they are governed by. To illustrate this hierarchy, descriptions of the various levels are given below.

2.6.1 Information Security Policy

This is the collection of broad but topical policies (centred on specific Information Security topics). Offis' Information Security Policies are organised in accordance with **ISO 27002, Information Technology – Security techniques – Code of practice for information security controls**, an international standard and is in compliance with other regulatory and compliance mandates where applicable. The Information Security Policies are contained in this document.

2.6.2 Information Security Standard and Processes

These are collections of standards and guidelines that are to be used to implement the given policy they reference. Standards may dictate a type of technology to use, but may stop before naming a particular product (depending on the policy and standard subject). Guidelines will detail the steps to take to fulfil the goals of a particular policy. Standards and Guidelines will clearly delineate where they apply.

2.6.3 Information Security Specific Configurations and Procedures

These are very specific details that support the implementation of the standards and guidelines given above. These will include specific products and configuration details, or step-by-step procedures to implement processes. These are highly localised and will apply to the environment for which they were written (e.g. configuration for Windows will differ to Linux). These will be published under separate titles where directed.

3. Policy

3.1 Information Security Policy Document

Offis Executive Management will provide direction for, approve, publish and communicate the merits of an Information Security Policy document. This document shall outline management's approach to Information Security as well as providing the organisation with a strong indication of the management's commitment to Information Security within Offis.

The purpose of this policy is to communicate the direction of the organisation's Information Security Program by providing relevant, accessible and understandable definitions, statements and explanations.

The Information Security Policy Document shall:

- Define information security as well as its importance in the organisation;
- Include a statement of management's intent for information security;
- Include a statement of management's goals and principles of information security;
- Explain the organisation's security policies, standards and compliance requirements including:
  - Compliance with regulatory, legislative and contractual requirements,
  - Security education and awareness commitment,
  - Consequences for security violations,
  - Commitment to well thought-out and effective business continuity management.
- Outline specific responsibilities for information security management to defined roles;
- Outline policies and procedures for reporting security incidents and deviations or exceptions;
- Be communicated to employees and relevant external parties

3.2 Review and Evaluation of Information Security Policy

The company information security officer shall be the owner of this Information Security Policy document. The owner of the document shall be responsible for maintaining and reviewing the policy based upon a defined review process. The policy shall be reviewed at least annually and updated in response to any changes that would affect the assumptions from the baseline risk assessment, such as significant security incidents, new vulnerabilities, new regulations or changes to the organisation's infrastructure.

The reviews shall include an assessment of the policy's effectiveness based upon:

- The nature, number and impact of recorded security incidents;
- Cost and impact of controls on business efficiency; and
- Effects of changes to technology

4. Organisation of Information Security

4.1 Internal Organisation

4.1.1 Roles and Responsibilities

The purpose of this policy is to protect all information assets within the organisation by allocating specific responsibilities for all such assets.

Each asset should have an "owner", who may delegate responsibilities, but remains ultimately responsible for the asset(s).

The asset owner shall:

- Identify and define all security processes for their asset(s);
- Document all security processes on their assets; and
- Clearly define and document all authorisation levels for their assets

4.1.2 Segregation of Duties

Conflicting duties and areas of responsibility are to be avoided and should be segregated, where possible or practical, in order to reduce opportunities for unauthorised or unintentional modification or misuse of the organisation's assets.

Where segregation is not possible, authorisation, monitoring of activities, audit trails or management supervision controls will need to be in place.

4.1.3 Contact with Authorities

Offis shall maintain a list of authorities, including law enforcement, regulatory bodies and supervisory authorities, which may be contacted as a result of an information security incident. Procedures must be in place to specify how security incidents should be reported, and when and by whom these authorities should be contacted.

Contacts with regulatory bodies shall also be used to prepare for changes in laws or regulations, which must be implemented by the organisation. Contacts with other authorities including utilities, emergency services, electricity suppliers, health and safety, and telecommunication providers must also be maintained for business continuity and contingency planning.

4.1.4 Contact with Special Interest Groups

Offis shall maintain appropriate contacts with special interest groups or other specialist security forums and professional associations as a means to improve in-house knowledge about best practices and stay up to date with relevant security information to the business. This will further assist in assessing the overall effectiveness of Offis' Information Security Policy.

Such contacts will additionally provide a means to receive early warnings of relevant alerts, advisories and patches pertaining to attacks and vulnerabilities, and gain access to specialist information security advice.

4.2 Mobile Devices and Teleworking

4.2.1 Mobile Computing

Offis institutes the following policies to ensure that business information is not compromised by use of such devices as notebooks, smartphones and tablets in an unprotected environment and to provide users with controls for and awareness of the potential risks.

Users of mobile computing devices shall be required to sign a statement of their understanding and compliance. This statement should be included in the policy acceptance letter signed during employee induction and yearly performance reviews.

4.2.1.1 Physical Protection of Mobile Devices

Users must reasonably ensure mobile devices are not left unattended and are physically secure at all times if they contain sensitive data. For example, mobile devices should never be left visible in a car, should always be carried on board aircraft and not placed in checked luggage, and should not be left on tables in public places if they will be out of sight.

4.2.1.2 Access Control

If a mobile device contains other than public Offis data, it must have some form of access control to access this information. If access to the device is not controllable, access to the data must be controlled.

4.2.1.3 Use of Encryption

If a mobile device contains sensitive Offis data, it must be encrypted on the storage drive. Encryption may be on a file-by-file basis, or on a volume-by-volume basis.

4.2.1.4 Protection from Viruses/Malicious Software

If capable, mobile devices shall run anti-virus software with current updates/definitions. All notebooks must use Offis-approved anti-virus software.

4.2.1.5 Backups

Users are strongly encouraged to back up their Offis data stored on mobile devices. Backup data must be protected and encrypted.

4.2.1.6 Connecting to Offis Corporate Network in Office

Users may only connect mobile devices that have been authorised by the company information security officer, and adhere to the Standard Operating Environment (SOE) for Staff Workstations policy, to the Offis corporate network. Direct physical connectivity to the Offis corporate network while simultaneously connected to an outside network through any form of network interface (modem, wireless, second Ethernet adapter) is not permitted. These devices must have current anti-virus software running and the user must be reasonably certain that no other malicious software is operating on the device. Users are encouraged to have Operations check their approved mobile devices before connecting to the Offis corporate network if they have reason to believe they may have come into contact with any malicious software, whether detected by anti-virus protection or not.

4.2.1.7 Connecting to Offis Corporate Network from Public Places

Remote connections to the Offis corporate network may be made by approved mobile devices at public places under the following provisions. Users must use an approved personal firewall, and have it running and actively filtering traffic when connecting to the Offis corporate network from public places. Users must also have current and active anti-virus software running before connecting. Remote connections will be made through VPN tunnels to safeguard the connection traffic. Connections from home networks may use a gateway firewall in place of the personal firewall, but one of the other must be operational and actively filtering traffic.

4.2.1.8 Connecting to Networks in Offis Data Centre

Same policy as “Connecting to Offis Corporate Network from Public Places”.

4.2.1.9 Wireless Connections

Offis users must use a personal firewall and anti-virus software (as discussed above) whenever connected to a wireless network. The use of WPA or greater privacy measures is encouraged where available.

4.2.2 Teleworking

Offis information resources cannot be compromised by those that access them from premises that are not under the control of the organisation by the following policies which define the conditions and restrictions for using teleworking. Teleworking refers to all forms of work outside of the office and data centre.

4.2.2.1 Authorisation for Remote Access

All teleworking (work that occurs remotely and requires access to the organisation’s information resources) shall be authorised by the company information security officer in accordance with the following rules:

- All teleworking will be specifically authorised
- The access to sensitive information shall be specifically authorised
- The storage of sensitive information shall be specifically authorised
- The work performed by the teleworking shall be specifically authorised
- The teleworking shall have adequate and secure communications equipment
- The teleworker shall be given access to support and maintenance services
- Communication requirements will be secure and in line with those required by the information to be accessed classification.

4.2.2.2 Applicability of Offis Policy during Teleworking

Users are responsible for any security breaches that occur as a result of their negligence in securing their personal remote systems. By using their own equipment, users are accepting responsibility to protect organisational information in accordance with policy. Offis reserves the right to audit and monitor any equipment used to process or store Offis information resources, regardless of ownership.

4.2.2.3 Remote Access Methods and Authentication of Connections

Users will employ only Offis approved remote access methods when connecting to the Offis corporate network or networks within Offis’ data centres and facilities. In addition, users connecting remotely will be authenticated before being allowed to connect, with users requiring high security privileges (such as Operations personnel) being authenticated using a two-factor method of authentication.

This provision applies equally to the connection to the Offis corporate network and connections to Offis information resources within the network. Only approved methods of system remote access will be allowed in accordance with IT standards and guidelines. All use of non-approved access methods, or approved access methods not utilising IT approved configurations and settings, will be subject to disciplinary procedures.

At no time, will commercial remote access services (such as LogMeIn) be allowed within Offis networks, systems, or home systems that store or process Offis information.

4.2.2.4 Remote Management of Systems

Remote management connections will only be made via encrypted connections (SSH, SSL, IPsec VPN, etc.). Where possible, remote connections must not allow logon via an elevated system account (i.e. root or administrator) directly. Administrators must log on with their user account and then change to the elevated privilege account, if required. This will ensure accountability and logging of unique IDs instead of shared administrative accounts.

5. Human Resource Security

5.1 Prior to Employment

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

5.1.1 Screening

Offis conducts background verification checks to ensure the safety of existing employees and to ensure that new employees possess the highest possible level of integrity and business ethics. All screening and supervision shall be in accordance with appropriate legislation and regulations.

5.1.1.1 Types of Background Checks

Offis requests the following types of background checks for all positions (employees and contractors):

- Character references (professional and personal)
- Verification of applicant's curriculum vitae
- Confirmation of claimed academic and professional qualifications
- Independent identity verification (passport, driver's licence, or similar document)
- Criminal records search (up to 5 years)

Offis requests a credit check for finance management and executive-level positions.

5.1.1.2 Who Requires a Background Check

All new employees of Offis require the successful completion of a background check prior to beginning their first day of work at Offis.

5.1.1.3 When to Request a Background Check

If the hiring manager is considering making an offer to a candidate, a background check should be requested any time after the first interview.

5.1.1.4 Who Decides if a Candidate Passes the Background Check

The hiring manager and company information security officer will make the determinations as to whether a candidate passes the Offis guidelines for the background check.

5.1.1.5 Collection and Handling of Background Check Information

Information on all candidates being considered for positions within the organisation should be collected and handled in accordance with The Privacy Act 1988. The candidates should be informed beforehand about the screening activities.

5.1.2 Terms and Conditions of Employment

Offis will state the employees' and contractors' roles and responsibilities for information security in the terms and conditions of employment.

Managers will provide each new employee with the employee's responsibilities for Information Security in the Employee Handbook. This handbook will contain information on Information Security policies, acceptable use, and ethics (direct information or instructions to obtain and read referenced policies). The employee's manager will provide the employee specific responsibilities that are particular to the specific position.

Disciplinary measures are covered in section 5.2.3 of this policy.

5.2 During Employment

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

5.2.1 Management Responsibilities

Management is responsible for ensuring that employees and contractors are:

- properly briefed on their information security roles and responsibilities prior to being granted access to confidential information or information systems
- provided with guidelines to state information security expectations of their role within the organisation
- motivated to fulfil the information security policies of the organisation
- able to achieve a level of awareness on information security relevant to their roles and responsibilities within the organisation
- conforming to the terms and conditions of employment, including the organisation's information security policy
- continuing to have the appropriate skills and qualifications, and are educated on a regular basis
- provided with an anonymous reporting channel to report violations of information security policies or procedures

5.2.2 Information Security Awareness, Education and Training

All employees will be appropriately trained on the organisation's Information Security policies and kept up-to-date on any additions or changes to the policies. Training is mandatory prior to receiving access to information or services.

The employee's manager is responsible for initial training and education on the organisation's security policies during the employee induction process. Employees should have recurring periodic refresher training on current threats, as well as material changes to policy.

When employees sign acknowledgements for complying with policy, these acknowledgements should include acknowledgment of initial training. The employee's manager will be responsible for the on-going policy education and training policy.

5.2.3 Disciplinary Process

In support of the Information Security Program, Offis will establish a formal disciplinary process for those who violate the organisation's security policies and procedures.

Disciplinary processes shall be documented by management and given to all employees and applicable third parties. Discipline for violating security policy or causing a security breach will be as appropriate, up to and including termination or possible criminal/civil charges.

If an employee is suspected of a breach of security, management shall be informed and the company information security officer, together with the manager of the person suspected, shall begin the investigation.

5.3 Termination and Change of Employment

Offis will ensure the organisation's interests are protected as part of the process of changing or terminating employment.

5.3.1 Termination or Change of Employment Responsibilities

A period is defined after the end of an employee's or contractor's employment whereby information security requirements, legal responsibilities, responsibilities within any confidentiality agreement, and the terms and conditions of employment continue and remain valid.

Responsibilities and duties still valid after termination of employment are stipulated in the employee's or contractor's terms and conditions of employment.

Changes of responsibilities or employment are managed as a combination of the termination of the current responsibility or employment and the initiation of the new responsibility or employment.

6. Asset Management

6.1 Responsibility for Assets

The purpose of this policy is to determine the protective controls associated with each Offis information asset and to provide a foundation for all employees (and contractors, third parties, etc.) to understand the security and handling of such assets.

6.1.1 Inventory of Assets

Offis will compile a list of all its information assets, and establish the relative value and importance of each asset.

An inventory of all assets and systems relevant in the lifecycle of information (creation, processing, storage, transmission, deletion, destruction) will be identified and documented, ensuring the following:

- All assets shall have an owner
- All assets shall be classified (see 6.2) based upon their value and importance to the organisation
- Assets will be categorised into logical categories such as information assets, software assets, physical assets and service assets

6.1.2 Ownership of Asset

Assets maintained in the inventory may be owned by individuals as well as other entities having approved management responsibility for the asset lifecycle (e.g. Operations).

A timely process to assign asset ownership is implemented, which occurs when assets are created or transferred to the organisation. The asset owner is responsible for the proper management of an asset over the whole asset lifecycle, including:

- ensuring that assets are inventoried
- ensuring that assets are appropriately classified and protected
- defining and periodically reviewing access restrictions/policies and classifications to important assets
- ensuring proper handling when the asset is deleted or destroyed
- delegating routine tasks for the assets (if applicable) but retaining owner responsibility

6.1.3 Acceptable Use of Assets

Employees and external party users using or having access to Offis assets are made aware of the information security requirements of the organisation’s assets associated with information and information processing facilities and resources. They are responsible for their use of any such assets and resources.

The Offis Pty Ltd Acceptable Use Policy provides the rules for the acceptable use of information and assets associated with information processing facilities, of which all employees and external party users must adhere to.

6.1.4 Return of Assets

All organisational assets in the possession of employees and external third party users shall be returned upon termination of their employment, contract or agreement.

A formal termination process includes the return of all previously issued physical and electronic assets owned by or entrusted to the organisation. In cases where the user purchases the organisation's equipment or use their own personal equipment, procedures to transfer or securely erase all relevant information from the equipment must be followed.

In cases where an employee or external party user has knowledge that is important to ongoing operations, that information shall be documented and transferred to the organisation.

During the notice period of termination, unauthorised copy of relevant information (e.g. intellectual property) by terminated employees and contractors is strictly prohibited.

6.2 Information Classification

Information classification is the process of assigning value to data in order to organise it according to its sensitivity to loss or disclosure. Offis shall ensure that all information assets are classified and protected in accordance with their importance to the organisation.

6.2.1 Classification of Information

All information assets are required to be classified and labelled in a manner that allows the asset to be readily identified to determine the handling and protection level for that asset. Assets other than information should also be classified in conformance with classification of information which is stored in, processed by or otherwise handled or protected by the asset.

Information shall be assigned a sensitivity classification by the owner or their nominees, in accordance with the following classification definitions:

- **Confidential**: Sensitive information requiring the highest degree of protection. Access to this information shall be tightly restricted based on the concept of need-to-know. Disclosure requires the information custodian's approval and, in the case of third parties, a signed confidentiality agreement. If such information was to be compromised, there could be serious negative financial, legal, or public image impact to Offis or Offis' members. Examples include member share information, employee performance reviews, product research data, etc.
- **Internal**: Information that is related to Offis business operations, but not available for public consumption. This information should only be disclosed to third parties if a confidentiality agreement has been signed. Disclosure is not expected to cause serious harm of Offis, and access is provided freely to all employees. Examples include policies and standards, operational procedures, etc.
- **Public:** Information that requires no special protection or rules of use. This information is suitable for public dissemination. Examples include press releases, marketing brochures, etc.

The company information security officer is responsible for maintaining the policy and ensuring the infrastructure exists to support this policy.

6.2.2 Labelling of Information

It is important that an appropriate set of procedures is defined for information labelling and handling in accordance with the classification scheme adopted by Offis. These procedures must cover information assets in physical and electronic formats.

System outputs containing confidential information shall carry an appropriate classification label (in the output).

The labelling should reflect the classification according to the rules established in 6.2.1. Items for consideration include printed reports, screen displays, recorded media, electronic messages, and file transfers.

All printed, handwritten, or other paper manifestations of confidential information shall have a clearly evident sensitivity label on the bottom of each page or a watermark that indicates the sensitivity classification.

6.2.3 Handling of Assets

For each classification, handling procedures should be defined to cover the following types of information process activity;

- Copying
- Storage
- Transmission by post, fax, and electronic mail
- Destruction

Unless it has specifically been designated as “Public”, or “Internal”, all Offis internal information shall be assumed to be confidential and shall be protected from disclosure to unauthorised third parties.

Access to every office, computer room, and work area containing confidential information shall be restricted, and employees shall take all reasonable steps to protect confidential information under their control from inadvertent disclosure.

Handling rules must include all parts of an asset’s life-cycle, from creation/installation through use and finally to destruction/disposal. Sensitive information or systems must be appropriately disposed of when no longer needed.

6.3 Media Handling

Offis shall prevent the unauthorised disclosure, modification, removal or destruction of information stored on media.

6.3.1 Management of Removable Media

Removable media should be managed through the implementation of procedures in accordance with Offis' information classification scheme and the following guidelines:

- The contents of any re-usable media that are no longer required and are to be removed from the organisation should be made unrecoverable;
- Authorisation should be required for media to be removed from the organisation and a record of such removals should be kept in order to maintain an audit trail;
- All media should be stored in a safe and secure environment, in accordance with manufacturers' specifications;
- Cryptographic techniques should be used to protect data on removable media if data confidentiality and/or integrity are important considerations;
- Where stored data is still needed, the risk of media degradation should be mitigated by transferring data to fresh media before becoming unreadable;
- Multiple copies of valuable data should be stored on separate media to further reduce the risk of data damage or loss;
- Where there is a need to use removable media, the transfer of information to such media should be monitored.

6.3.2 Disposal of Media

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

Such formal procedures should be established to minimise the risk of confidential information leakage to unauthorised persons. This includes identifying items that might require secure disposal, using such disposal methods as incineration, shredding or secure data erasure prior to re-use, and logging disposal of sensitive items for auditing purposes.

6.3.3 Physical Media Transfer

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

This shall be achieved through:

- the use of reliable transport or couriers as authorised by management;
- the development of procedures to verify the identification of transporters or couriers;
- the use of sufficient packaging to protect the contents from any physical damage during transit and in accordance with any manufacturers' specifications
- maintenance of logs to identify the content of media and record the times of transfer to the transit custodians and receipt at the destination

7. Access Control

7.1 Business Requirements of Access Control

7.1.1 Access Control Policy

Offis shall establish and document access control rights and rules for each user or group of users. Access to information and information services will only be given on the basis of business and information security requirements.

Access to information assets will be given on a need-to-know or need-to-use basis, based upon the security requirements and business requirements of individual business applications. Access to information shall be provided in a manner that aims to protect the confidentiality and integrity of that information without compromise to associated information or raw data.

Data owners shall review access control rights for users and groups of users on an annual basis to ensure that all access rights are authorised and remain appropriate, and that no unauthorised privileges have been gained.

All forums where confidential information may be discussed and where non-Offis employees are present shall be preceded by a determination that all parties are authorised to receive the information and the appropriate categorisation of that information.

Access will be given that is consistent with the security levels and classifications, consistent with legislation and contractual obligations for confidentiality.

Access rights in a networked environment will recognise all connection types available.

All users and groups of users shall receive a clear statement as to the access policy and as to the requirements met by these access controls.

Originators of confidential information shall decide who will be permitted to gain access to that information, and shall specify the uses for that information.

Administrator access to production systems will be limited to only those with a justified business requirement for such access. Developers and other application personnel will not have access to the underlying operating system on production systems, unless deemed an emergency, and then with access only granted for the time necessary.

Access rules will specifically differentiate between those rules that are optional or conditional and those that are always to be enforced.

Access rules will be declarative statements such as “access is forbidden unless specifically permitted” instead of “access is generally permitted unless forbidden”.

Access rules will differentiate between permissions that are granted by the information system and those permissions that must be granted by an administrator.

Access rules will differentiate between those rules that require approval and those that do not.

Access rules will consider changes in classifications that are automatic and those classification changes that must be initiated by an administrator.

Access rules for each system will be developed in accordance with the Information Classification guidelines commensurate with the information's sensitivity.

7.1.2 Access to Networks and Network Services

Users shall only have access where there is a specific business requirement and the access has been specifically authorised. Users will be granted specific access to networks that they are permitted to access. Users may not access networks that they are not given specific authorisation to access.

Information Security shall control and manage the rules, policies and procedures for users accessing network connections and network services.

Third parties that must deploy non-Offis controlled systems must be specifically approved by the company information security officer.

7.1.2.1 Network connection controls

Highly sensitive systems will have network access controls in place to prevent unauthorised connections from inside, or outside, Offis. This is in addition to any application or system access controls. Restrictions will be consistent with the organisation's access control policy.

Network controls shall be configured to allow only network traffic required by the business to enter or leave Offis networks. The network security team shall work with management to determine those business requirements.

7.1.2.2 User authentication for network access

All remote users will be authenticated before they are permitted to access information resources. Users will be given remote access only when their job function requires it. Any non-employee who receives approval for remote access must be to access specific systems only.

The system owners, in coordination with the company information security officer, shall select from the following options based upon the results of the risk assessment:

- Cryptography
- Hardware/software tokens
- Challenge/response protocol
- Dedicated private lines
- Network user address checking

7.2 User Access Management

7.2.1 User Registration and De-registration

A formal user registration and de-registration process must be used for gaining access to multi-user systems. This process must protect and maintain the security of access to the organisation's information resources through the complete life-cycle of the user.

A user's account and password is the primary means of verifying a user's identity. The allocation of passwords will be a formal management process.

Each person accessing an Offis multi-user based information system shall utilise a unique Offis-assigned user ID and private password.

IT operations will periodically check for redundant user IDs and ensure that redundant IDs are not issued more than that required. Administrators may have a privileged and a non-privileged account on the same system, but an average user should not have two different non-privileged accounts on the same systems without a valid business reason.

7.2.2 User Access Provisioning

Access to Offis confidential information shall be provided only after the authorisation of the information owner has been obtained.

System owners and/or management shall grant access rights. Formal records of all access rights for each system shall be maintained.

Contractors and third party contracts should contain the rights of access and sanctions if unauthorised attempts at access are made.

Service providers shall be made aware of policy not to provide access to users until specific authorisation has been given.

Access rights shall immediately be removed or modified when a user leaves the organisation or changes jobs.

7.2.3 Management of Privileged Access Rights

User rights shall be granted using the least-privilege methodology, based on business needs and security requirements.

All privileges shall be granted only with formal authorisation. This authorisation shall be accomplished along with user ID authorisation. All privileges that are granted will be documented. No privileges shall be granted until authorisation is complete.

Elevated privileges should be assigned to a different user ID than that used for normal business use. Administrators should only use their elevated privilege accounts when conducting activities that actually require them. Elevated privileges must only be assigned to system administrators and not normal users.

Wherever possible, system routines should be developed and used instead of privileges.

7.2.4 Management of Secret Authentication Information of Users

Users will sign a statement in their terms and conditions of employment that they will keep their personal or group passwords confidential. This may be done as part of the overall acceptance of policies.

Users will be responsible for the secure storage of their passwords.

Users will be granted initial temporary passwords and will be forced to change them immediately. Initial passwords will be unique for each user. Temporary passwords will only be granted with positive identification of the user.

Passwords will be given in a secure manner, and never in plain text by email.

7.2.5 Review of User Access Rights

Users' access rights will be reviewed at regular intervals. Managers will review their employee's rights to ensure they are consistent with their present job function. IT Operations will review user rights to ensure that elevated privileges have not been granted without authorisation, and that accounts that have not been used recently or belong to terminated employees are deactivated or purged.

User access rights shall be reviewed at least every six months. Privileged access rights shall be reviewed every three months to ensure that all are authorised and remain appropriate and that no unauthorised privileges have been gained.

7.3 User Responsibilities

7.3.1 Use of Secret Authentication Information

Offis has established a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

All Offis employees (including contractors and vendors with access to Offis systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any Offis facility, has access to Offis networks, or stores any non-public Offis information.

All users will keep their passwords confidential and store them securely (i.e. not on a computer or on paper unless they can be protected).

Users will be made aware of good security practices and the requirement to use good security practices with their passwords. All passwords are to be treated as confidential Offis information and should not be shared with anyone, including administrative assistants.

Password requirements:

- If an account or password is suspected to have been compromised, report the incident to the company information security officer and change all passwords
- Regular passwords shall be changed at least every 90 days
- Privileged passwords shall be changed every 90 days

- Shared privilege passwords (i.e. root, administrator, etc.) should be changed every 90 days or whenever someone with administrator-level access leaves the organisation
- Temporary passwords will be changed at first log-on
- Systems shall be configured to lock user accounts in the event of five consecutive unsuccessful login attempts. System administrators may reset locked accounts.
- Passwords will not be stored on a computer or used in a macro for sign-on
- Do not use the "Remember Password" feature of applications
- Passwords should not be written down or stored unencrypted on any computer or device
- Passwords will be at least 8 non-sequential characters long
- Passwords will be composed of alpha-number characters
- Passwords will contain at least 3 of the characteristics below:
    - alphabet character
    - upper case letter
    - number
    - non-alpha-numeric character (special character)

7.4 System and Application Access Control

7.4.1 Information Access Restriction

To safeguard applications, Offis will restrict access to business information and application systems on a need-to-know basis.

Menus and documentation shall be edited so the users only view data or menus that they are authorised to view.

Users' rights shall be based on a least-privileged basis so that they are limited to only those functions to which they are authorised (read, write, delete and execute). Users' rights shall be reviewed on a periodic basis to ensure that no user or group has excessive privileges.

Outputs available to users are limited to those to which they are authorised.

Sensitive outputs shall be controlled and limited to specific terminals and/or printers. Sensitive outputs must be controlled and limited to specific users who have a valid business need.

Periodic reviews will be performed to ensure that outputs of sensitive information are required by the business. Any extraneous output of sensitive information will be removed.

7.4.2 Secure Log-on Procedures

All users shall be identified and authenticated with the minimum of a unique identification and a password before access to systems and applications is granted. This will minimise the opportunity for unauthorised access to information resources by providing a means of user authentication. If access to the operating system is not necessary, such as when the user has access to an application (only) running on the system, then operating system access must not be given to the user.

If operating system access is necessary, such access will abide by the following rules:

- All users shall have a unique user account (see 7.2.1)
- All users shall have a unique password (see 7.2.4)
- Users' passwords will give no indication to their privilege level

Additional authentication technique(s) will be used in combination with user IDs to provide further security in authentication, including:

- Passwords (see 7.2.4 and 7.4.3)
- Cryptographic and authentication protocols (see 10.1)
- Smart tokens
- Biometrics

Log-on procedures should not display system or application identifiers until the log-on process has been successfully completed.

A general notice should be displayed at log-on time for higher privilege log-ons, warning that the system or application should only be accessed by authorised users.

There shall not be any help messages provided during log-on procedures that would aid an unauthorised user.

Passwords shall not be displayed when being entered.

Inactive sessions should be terminated 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.

Connection times should be restricted to provide additional security for high-risk applications and reduce the window of opportunity for unauthorised access.

7.4.3 Password Management System

All passwords for systems and applications must be individual, effective, and of sufficient quality to deter compromise. Systems and applications must be configured to programmatically enforce these rules if available. In the absence of programmatic enforcement, the user will be responsible for enforcing these rules themselves. See 7.3.1 for more information on passwords.

Furthermore, a password management system should:

- enforce the use of individual user IDs and passwords to maintain accountability;
- allow users to select and change their own passwords and include a confirmation procedure to allow for input errors;
- not store and transmit passwords in clear text;
- not display passwords on the screen when being entered;
- maintain a record of previously used passwords and prevent re-use;
- keep password files separate from application system data;
- enforce regular password changes and as needed;
- force users to change their passwords at the first log-on

7.4.4 Use of Privileged Utility Programs

Utility programs that can override system and application controls should be restricted and tightly controlled.

The use of utility programs should be authorised, logged and limited. Authorisation levels should be defined and documented.

Utility programs should not be available to users who have access to applications on systems where segregation of duties is required.

7.4.5 Access Control to Program Source Code

Access to program source code shall 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.

Program source libraries should not be held in operation systems, and should be managed according to established procedures.

An audit log shall be maintained of all accesses to program source libraries,

Maintenance and copying of program source libraries should be subject to strict change control procedures.

8. Cryptography

8.1 Cryptographic Controls

8.1.1 Policy on the use of Cryptographic Controls

The purpose of this policy is for Offis to assess the appropriateness of cryptography in the organisation and if deemed appropriate, implement policies, standards and controls for its proper and effective use.

Only Offis-approved uses of cryptography (encryption of any form) are allowed. This includes the methods of use (disk encryption, digital signatures, etc.) as well as algorithms or key strengths to be used.

Information to consider in the use of any encryption product includes:

- General principles under which business information should be protected
- The approach to key management, including protection of keys and recovery of encrypted information in the case of lost, compromised or damaged keys
- The determination of the appropriate level of protection in terms of type, strength and quality of encryption algorithm required
- Roles and responsibilities for implementation
- Roles and responsibilities for key management
- Implementation of policies for use throughout the organisation
- Impact of using encrypted information on controls that rely upon content inspection

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

8.1.1.1 Confidentiality

Offis considers the use of encryption appropriate for protecting sensitive or critical information.

A risk assessment will be performed for any highly sensitive information, and will include:

- The need for encryption;
- The implementation of encryption;
- Policies for encryption;
- The appropriate level of sophistication of the encryption algorithms chosen;
- The appropriate lengths of keys to be used

8.1.1.2 Integrity

Offis will consider the appropriateness of the use of digital signatures to protect and authenticate the integrity of electronic documents.

Risk assessments performed will cover key security, key management, use of different keys than those used with encryption, and relevant legislation on the use of and legal standing of digital signatures.

8.1.1.3 Non-repudiation Services

In support of digital signatures, Offis will consider non-repudiation services where necessary. A mechanism should be in place for the resolution of disputes regarding the substantiation of a receipt of a digitally signed document, prior to the dispute.

The identification and ownership of digital certificates and private keys should be established, and private keys shall be safeguarded.

8.1.2 Key Management

To ensure the protection of cryptographic keys, both public and private keys, Offis will enact policies and procedures concerning key management. Key management policies and procedures will protect all keys from modification, destruction and unauthorised disclosure that could lead to a compromise in the authenticity, integrity and confidentiality of information.

A management plan and system shall be in place for the use of public and private keys that ensures the confidentiality and integrity of the private keys.

Keys shall be changed immediately if it is suspected that the keys were compromised. This may entail re-encrypting stored data with new secret or public keys.

All application systems that are using cryptography shall have different keys, and the application owner shall be responsible for generating and managing the keys in accordance with this policy and any applicable standards and guidelines published by Offis.

A list of systems that require keys shall be kept and evaluated periodically to ensure the accuracy and relevancy of the list.

Keys will be distributed and stored in a secure manner. Revoked keys will be maintained in a secure manner to cover eventualities where data may have been encrypted with these keys before their revocation and have not been switched to new keys.

Standards, procedures and methods for key management shall be established to include the following:

- Secure procedures for key obtaining and storing keys
- Establishing and documenting the rules for changing and updating keys
- Procedures for dealing with compromised keys or keys that have been revoked or deactivated
- Secure procedure for destroying keys, including how and by what method
- Secure procedures for key management business continuity including recovery of lost or corrupted keys, supplier provisions for system loss, and archiving keys for achieved or backed-up information afters keys have been changed
- Secure procedures for legal issues including requests for access to cryptographic keys in court proceedings, legal agreements with suppliers of cryptographic services, and legal agreements with trading partners
- Secure procedures for establishing and defining the relationship between Offis and a trusted third party certification authority for the protection of public keys, if used

9. Physical and Environmental Security

9.1 Secure Areas

9.1.1 Physical Security Perimeter

Security perimeters shall be defined, with the siting and strength of each perimeter dependent upon the security requirements of the assets within the perimeter and the results of a risk assessment.

The perimeters of a building or site containing information processing facilities shall by physically sound; 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; doors and windows should be locked when unattended and external protection should be considered for windows, particularly at ground level.

A managed reception area or other means to control physical access to the site or building shall be in place, with access restricted to authorised personnel only.

All fire doors on a security perimeter shall be alarmed, monitored and tested to establish the required level of resistance in accordance with suitable regional, national and international standards.

Information processing facilities managed by the organisation should be physically separated from those managed by external parties.

9.1.2 Physical Entry Controls

Physical entry controls will be used to protect all secure areas. These controls will be designed to prevent unauthorised access, damage or interference to the business processes that take place within the area. Physical security controls apply to any Offis owned or controlled facility, including temporary locations.

The date and time of entry and departure of visitors of secure areas should be recorded. All visitors should be supervised and 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.

Access to sensitive information and information processing facilities will be restricted to authorised persons only. Authentication controls will be used to authorise and validate entry. A log of all access will be maintained as appropriate for the sensitivity of the information resources therein.

Controls to restrict access will ensure that unauthorised persons do not have easy physical access to the facilities, and such access is detected and the appropriate personnel notified if a breach occurs.

Employees will notify security personnel of unfamiliar people who are unescorted or not showing visible identification.

Access rights will be given on a least-privilege basis and will be reviewed periodically and updated where necessary.

9.1.3 Securing Offices, Rooms and Facilities

All offices, rooms and facilities that contain other than public information resources will be physically protected accordingly to prevent unauthorised access, damage or interference to the business processes. Where possible, systems shall monitor the physical security of key facilities.

Rooms containing sensitive assets will be locked when not in use. Windows and doors will be kept locked and have protection from intrusion or environmental factors.

The use of buildings that contain sensitive materials or processing facilities will be unobtrusive and not marked in such a way that gives the public any indication of the presence of information processing facilities.

Directories and telephone books that provide information on locations of confidential information processing facilities shall be secured from unauthorised access.

9.1.4 Protecting Against External and Environmental Threats

Hazardous or combustible materials shall be stored securely at a safe distance from secure facilities.

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

9.1.5 Working in Secure Areas

The existence of, or activities within, a secure area shall only be made aware to personnel on a need-to-know basis.

Unsupervised work performed in secure areas should be avoided for safety reasons and to prevent opportunities for malicious activities.

Unauthorised use of photographic, video, audio or other recording equipment is not allowed.

9.1.6 Delivery and Loading Areas

Delivery and loading areas, and other access points whereby unauthorised persons could enter the premises from outside the building, shall be controlled and, if possible, isolated from information processing facilities.

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.

Incoming material should be inspected and examined for explosives, chemicals or other hazardous materials before it is moved from a delivery and loading area.

9.2 Equipment

9.2.1 Equipment Siting and Protection

Equipment should be sited to minimise unnecessary access into work areas.

Information processing facilities used by Offis to handle sensitive data shall be positioned carefully to reduce the risk of information being viewed by unauthorised persons during their use.

Storage facilities shall be secured to avoid unauthorised access, with items requiring special protection to be further safeguarded.

The risk of potential physical and environmental threats shall be minimised with appropriate controls. Such threats may include theft, fire, explosives, smoke, water, dust, vibration, chemical effects, electrical supply interference, communications interference, electromagnetic radiation, and vandalism.

Guidelines for eating, drinking and smoking in proximity to information processing facilities shall be established. Environmental conditions, including temperature and humidity, should be monitored for conditions that could adversely affect the operation of information processing facilities.

9.2.2 Supporting Utilities

Offis equipment is dependent on supporting utilities including electricity, telecommunications, ventilation and air conditioning. Such utilities must conform to equipment manufacturers' specifications and local legal requirements.

Supporting utilities should be appraised regularly for their capacity to meet business growth and interactions with other supporting utilities. Inspections and testing shall be performed regularly to ensure their proper functioning.

Where possible, redundancies shall be obtained as appropriate to the criticality of equipment for which the utilities support.

9.2.3 Cabling Security

Power and telecommunications cabling carry data or supporting information services shall be protected from interception, interference or damage.

Power and telecommunications lines into information processing facilities should be underground where possible, or subject to adequate alternative protection.

Power cables should be segregated from communications cables to prevent interference.

For sensitive or critical systems, further controls should be considered, including, but not limited to, locked rooms or boxes at inspection and terminations points, electromagnetic shielding to protect cables, regular physical inspections, and controlled access to patch panels and cable rooms.

9.2.4 Equipment Maintenance

The availability and integrity of equipment shall be ensured through the use of correct maintenance, in accordance with supplier's recommended service intervals and specifications.

Only authorised maintenance personnel shall carry out repairs and service equipment, with records kept of all suspected or actual faults, and of all preventative and corrective maintenance performed. Equipment shall be inspected to ensure that it has not been tampered with and will not malfunction prior to placing equipment back into operation after maintenance.

When equipment is scheduled for maintenance, appropriate controls shall be implemented to take into account whether this maintenance is to be performed by Offis personnel or third parties. Where necessary, confidential information should be cleared from the equipment or the maintenance personnel should obtain sufficient clearance.

All maintenance requirements imposed by insurance policies shall be complied with.

9.2.5 Removal of Assets

Authorisation shall be obtained prior to taking Offis equipment, information or software off-site.

Offis employees and external party users who have authority to permit off-site removal of assets shall be identified.

Where necessary and appropriate, assets should be recorded as being removed off-site and recorded when returned.

9.2.6 Security of Equipment and Assets Off-Premises

There are different risks to consider when working outside the organisation’s premises, and as such, off-site assets and equipment shall be protected accordingly.

The use of any information storing and processing equipment outside Offis premises, including Offis owned equipment and privately-owned equipment used on behalf of Offis, should be authorised by management.

Equipment and media taken off Offis premises shall not be left unattended in public places. Off-premises locations such as home-working, teleworking and temporary sites should have suitable controls applied as appropriate and determined by risk assessment. Controls may include lockable cabinets, clear desk policy, access controls for computers, and secure communication with the office.

9.2.7 Secure Disposal and Re-Use of Equipment

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

Storage media containing confidential or copyrighted information shall be physically destroyed, or the contained information shall be destroyed, deleted or overwritten using techniques to make the original information irretrievable.

Whole-disk encryption should also be used as a mitigating control for reducing the risk of disclosure of confidential information when equipment is disposed of or redeployed.

9.2.8 Unattended User Equipment

Offis users are responsible for protecting unattended equipment in accordance with organisational security requirements and procedures.

Active sessions shall be terminated or secured by an appropriate session locking mechanism when finished. Users should log-off from applications or network services when no longer needed.

Computers or mobile devices should be secured from unauthorised use by a key lock, or equivalent control such as password, when not in use.

9.2.9 Clear Desk and Clear Screen Policy

Offis adopts a clear desk policy for papers and removable storage media, and a clear screen policy for information processing facilities.

Sensitive or critical business information on paper or electronic storage media should be locked away when not required.

Computer and terminals shall be left logged off or protected with a screen and keyboard locked mechanism controlled by a password, token or similar user authentication mechanism when unattended or not in use.

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

10. Operations Security

10.1 Operational Procedures and Responsibilities

10.1.1 Documented Operating Procedures

All standard operating procedures shall be formally documented and maintained to ensure the correct and secure operations of all information processing facilities.

Documented procedures and operational instructions shall be in place for activities associated with information processing and communication facilities, including:

- Information processing and handling;
- System installation and configuration;
- Scheduling requirements, including system interdependencies, earliest job start and latest job completion times;
- Instructions for error handling and exceptions, during job execution;
- Operational and support contacts for technical difficulties;
- Output instructions for confidential or sensitive output, including security disposal of output from failed jobs;
- System restart and recovery procedures in the event of system failure;
- Management of audit trail and system log information;
- Monitoring procedures;
- Backups.

10.1.2 Change Management

Formal management responsibilities and procedures to control changes to the organisation, business processes, information processing facilities and systems that affect information security will be established and followed.

Prior to any operational change, there shall be a risk assessment that:

- Identifies and records significant changes;
- Plans and tests changes;
- Assesses the potential impact of such changes;
- Verifies that information security requirements have been met.

Formal approval procedures shall be in place for proposed changes, with communication of change details to all relevant persons. Fall-back procedures and responsibilities shall be established for aborting and recovering from unsuccessful changes and unforeseen events. An emergency change process should also be in place to enable quick and controlled implementation of change needed to resolve an incident (see 14.1).

10.1.3 Capacity Management

To limit disruption to the network, applications, and business functions, Offis will monitor system capacity and plan for future capacity needs in sufficient time to procure systems resources prudently. This will ensure adequate resources are available and reduce the possibility of system overload.

Capacity requirements should be identified, with consideration on the business criticality of the concerned system.

Providing sufficient capacity shall be achieved by increasing capacity or reducing demand.

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

10.1.4 Separation of Development, Testing and Operational Environments

Offis shall separate development, testing and operational environments to reduce the risks of unauthorised access or changes to the operational environment. The level of separation that is necessary to prevent operational problems should be identified and implemented.

Rules for the transfer of software from development to operational status should be defined and documented. Development and operational software should run on different systems or computer processors and in different domains or directories.

Changes to operational systems and applications should be tested in a testing or staging environment prior to being applied to operational systems. Other than in exceptional circumstances, testing should be avoided on operational systems. Users should use different user profiles for operational and testing systems.

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

10.2 Protection from Malware

10.2.1 Controls Against Malware

Protection against malware shall be based on malware detection and repair software, information security awareness, and appropriate system access and change management controls.

A formal policy prohibiting the use of unauthorised software shall be established (10.6.2).

Controls shall be implemented to prevent or detect the use of unauthorised software or suspected malicious websites.

Vulnerabilities that could be exploited by malware shall be reduced through technical vulnerability management.

Regular reviews of the software and data content of system supporting critical business processes should be conducted, with the presence of any unapproved files or unauthorised amendments formally investigated.

Malware detection and repair software shall be installed and regularly updated to scan computers and media on a routine basis. The malware scan shall be performed on any files received over networks or via any form of storage medium, and on electronic mail attachments at the mail servers and end users' computers. Web pages shall also be scanned for malware.

10.3 Backup

10.3.1 Information Backup

Offis will regularly back up adequate copies and generations of business information, software and system images in accordance with an agreed backup policy. Regular testing should be performed to ensure the quality and usability of backed up resources.

The backup policy shall maintain the availability and integrity of essential information resources in the case of failure or disaster by retaining up-to-date backups that are stored at a distance sufficient to escape damages that might occur at the primary site.

The extent 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.

Restoration procedures shall be documented and tested to ensure that they are effective and comply with restoration time requirements.

Backup media shall be tested annually to ensure that they can be relied upon for emergency use when necessary. Testing shall not overwrite the original media in case the backup or restoration process fails and causes irreparable data damage or loss.

In situations where confidentiality is of importance, backups shall be protected by means of encryption.

To protect Offis' information resources from loss or damage, personal computer users are responsible for regularly backing up the information on their workstation computers to their respective network file shares that are assigned to them by IT Operations. These shares are backed up daily to secure media for disaster recovery purposes.

10.4 Logging and Monitoring

10.4.1 Event Logging

Offis will capture and review all security-relevant event logs, user activities, exceptions, faults, and information security events.

Event logs will be retained for at least one year with at least three months of online retention.

Event logs shall contain:

- User IDs
- Dates, times and details of key events, including log-on and log-off
- Terminal or device identity (system name and network address)
- Successful and rejected system access attempts
- Successful and rejected data access attempts
- User of elevated privileges
- Confidential files accessed and kind of access
- Network addresses and protocols
- Alarms raised by the access control system
- Activation and de-activation of protection systems, such as anti-virus systems and intrusion detection/prevention systems

Event logs can contain sensitive data and personally identifiable information, and as such, appropriate privacy protection measures shall be taken.

Where possible, system administrators should not have permission to erase or de-activate logs of their own activities.

10.4.2 Protection of Log Information

Offis shall protect against tampering and unauthorised access to logging facilities and log information.

Controls shall protect against:

- alterations to the message types that are recorded;
- log files being edited or deleted;
- storage capacity of the log file media being exceeded, resulting in either the failure to record events or over-writing of past recorded events.

10.4.3 Administrator and Operator Logs

The activities of system administrators and system operators shall be logged, with the logs protected and regularly reviewed. This will ensure that accountability is maintained for privileged users.

10.4.4 Clock Synchronisation

Offis will use a common method and single reference time source to ensure that all clocks of relevant information processing systems are synchronised. This will ensure the accuracy of the audit logs, and protect the integrity and credibility of any logs that might be needed for legal, regulatory, contractual, standards compliance, and internal monitoring requirements.

All computers with real-time clocks shall be set to one reference time standard for use throughout the organisation.

10.5 Control of Operational Software

10.5.1 Installation of Software on Operational Systems

Offis shall implement procedures to control the installation of software on operational systems.

The updating of operational software, applications and program libraries should only be performed by trained administrators upon appropriate management authorisation.

Operational systems should only hold approved executable code and not development code or compilers.

Applications and operating system software shall only be implemented after extensive and successful testing covering usability, security, effects on other systems, and user-friendliness and should be carried out on separate systems (see 10.1.4).

A configuration control system should be used to keep control of all implemented software as well as system documentation.

A rollback strategy should be in place before any changes are implemented.

Previous versions of application software should be retained as a contingency measure.

Vendor supplied software used in operational systems should be maintained at a level supported by the supplier to avoid 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. Software patches should be applied when they can help to remove or reduce information security weaknesses (see 10.6).

10.6 Technical Vulnerability Management

10.6.1 Management of Technical Vulnerabilities

Effective technical vulnerability management can reduce risk to Offis' computing environment by verifying that systems or network devices are using acceptable patch levels, are not running unnecessary services, and do not have default passwords.

Offis shall 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.

Once a potential technical vulnerability has been identified, the associated risks and required actions to be taken should be identified. Depending on the urgency for action, the action taken can be carried out according to change management controls (see 10.1.2) or by following information security incident response procedures (see 14.1.5).

The risks associated with installing a patch should be assessed with respect to the risks posed by the vulnerability.

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.

In lieu of an unavailable patch, other controls will be considered, including disabling services or capabilities related to the vulnerability; adapting or adding access controls; increasing monitoring to detect actual attacks; and raising awareness of the vulnerability.

Systems at high risk shall be addressed with a higher priority. Any system containing (or accessing systems that contain) confidential data shall be subjected to internal vulnerability scans at least on a monthly basis.

Internet facing systems will be subjected to external vulnerability scans by a trusted third party on a case-by-case basis.

10.6.2 Restrictions on Software Installation

Offis shall define and enforce strict policy on which types of software users may install.

The principle of least privilege is applied, and only certain users with the required privileges may have the ability to install software. Offis shall identify what types of software installations are permitted, and grant privileges based on the roles of the users concerned.

Offis shall also identify what type of software installations are prohibited. Software that is only for personal use or whose pedigree with regards to being potentially malicious is unknown or suspect will not be permitted for installation.

10.7 Information Systems Audit Considerations

10.7.1 Information Systems Audit Controls

Any party conducting audits of information systems will carefully plan, agree upon, and expedite system audits so as to minimise the risk of disruptions to operational business processes. This will ensure the organisation's security requirement compliance while maximising the confidentiality, integrity and availability of the organisation's information resources.

The scope and requirements of all audits shall be controlled and agreed to by management.

Access to any files should only be read-only, with access beyond read-only allowed only for isolated copies of system files, which shall be approved by the company information security officer. If isolated copies of systems files are used, the files shall be erased as soon as the audit is completed.

Requirements for special or additional processing shall be identified and agreed upon by appropriate management.

Audit tests that could affect system availability should be run outside business hours.

All access shall be monitored and logged to produce a reference trail.

11. Communications Security

11.1 Network Security Management

11.1.1 Network Controls

Offis shall implement strict controls on the organisation's networks to ensure the safeguarding of information and protection of the organisation's infrastructure. Controls shall ensure the security of data in networks and protect the connected services from unauthorised access.

All procedures and responsibilities for the management of networking equipment shall be established.

Network access controls shall be observed for networks connected to public networks.

Appropriate logging and monitoring should be applied to enable recording and detection of actions that may affect, or are relevant to, information security.

The company information security officer will closely coordinate network management activities to ensure that controls are consistently applied across the information processing infrastructure.

11.1.2 Security of Network Services

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

Network services include the provision of connections, private network services and value added networks and managed network security solutions such as firewalls and intrusion detection systems.

Security features of network services may include technology applied for security of network services (such as authentication, encryption and network connection controls) and procedures for the network service usage to restrict access to network services or applications.

Any necessary security features, service levels and management requirements for network services shall be identified, and network service providers should implement these measures.

11.1.3 Segregation in Networks

Network controls must segregate groups of information services, users and information systems when interconnecting networks to customers, partners or other third parties.

Network segregation controls will be selected on the basis of risk assessment; cost and impact of incorporating suitable network technology. External connections must terminate in some form of controlled network (DMZ or similar) and must be subject to security controls. There shall be no direct connection between the Offis corporate network and any third party.

Based on site risk assessments, internal segregation of sites or networks within sites may be warranted. Development and testing networks/systems must be segregated from the rest of the internal network to prevent malfunctions in software from impacting the rest of the network.

Offis will separate development and production environments to prevent unfinished or malfunctioning software from affecting the business network. Only IT Operations approved systems will be connected to production environments, and only after the systems have fulfilled acceptance criteria.

11.2 Information Transfer

11.2.1 Information Transfer Policies and Procedures

Formal policies, procedures and controls shall be put in place when information is to be transferred within an organisation and with any external entity. They shall cover:

- Protection of transferred information from interception, copying, modification, misrouting and destruction;
- Detection of and protection against malware that may be transmitted through the use of electronic communications;
- Acceptable use of communication facilities;
- Responsibilities and liabilities in case of loss or compromise of data;
- Use of cryptographic techniques;
- Legal responsibilities for copyright protection, ownership and data protection;
- Retention and disposal guidelines for all business correspondence, including messages, in accordance with legislation and regulations;
- Advising personnel to take appropriate precautions not to reveal confidential information.

11.2.2 Agreements on Information Transfer

Agreements shall address the secure transfer of business information between the organisation and external parties.

The agreements should include management responsibilities for controlling and notifying transmission, dispatch and receipt, and procedures to ensure traceability and non-repudiation.

There shall be responsibilities and liabilities defined in the event of information security incidents such as loss of data.

An agreed labelling system for sensitive or critical information shall be established (see 6.2). Special controls are required to protect sensitive items, including the use of cryptography.

11.2.3 Electronic Messaging

Electronic messages shall be protected from unauthorised access, modification or denial of service commensurate with the classification scheme adopted by Offis.

Messaging services shall ensure correct addressing and transportation of messages.

External public messaging services such as instant messaging, social networking or file shared shall require approval to be obtained prior to use.

11.2.4 Confidentiality or Non-Disclosure Agreements

Offis expects that information disclosed to Offis employees will be treated with the appropriate level of confidentiality. Except as required by law, information concerning the company's business is not to be discussed with competitors, outsiders, or the media. Employees are prohibited from forwarding emails containing information on the company's business to anyone outside of the company or otherwise transmitting company-confidential information outside of the company. Failure to honour this confidentiality requirement may result in disciplinary action, up to and including termination of employment.

Employees may have access to Offis' confidential and/or proprietary information, including information concerning customers, suppliers and fellow employees. It is imperative that no employees disclose such information in any inappropriate ways, and that such information be used only in the performance of regular job duties.

Offis requires confidentiality or non-disclosure agreements from all employees and third party staff not otherwise covered by third party contracts before access to sensitive information or systems will be allowed. Agreements will be reviewed and signed by the staff member when there is any change to the employment contracts, or prior to leaving the organisation.

12. System Acquisition, Development and Maintenance

12.1 Security Requirements of Information Systems

12.1.1 Information Security Requirements Analysis and Specification

Information security requirements should be identified and included in the requirements for new information systems or enhancements to existing information systems.

Risks assessments shall be performed to evaluate the security requirements for new systems or upgrades.

System owners, in conjunction with the company information security officer, shall specify the security requirements of all new implementations prior to their final approval to ensure:

- The controls and requirements will reflect the sensitivity and business value of the information assets involved
- Vulnerability scans and/or penetration tests will be run against systems to ensure security controls are in place, patch levels are current, and unnecessary services are not running.

12.2 Security in Development and Support Processes

12.2.1 Secure Development Policy

Security shall be considered in the software development methodology, with secure coding guidelines followed for each programming language used. Secure repositories shall also be used.

If development is outsourced, assurance shall be obtained so that the external party complies with requirements for secure development.

12.2.2 System Change Control Procedures

Software development at Offis will utilise formal change control procedures for any changes to systems within the development lifecycle. This process shall be integrated with operational change control procedures.

Programmers shall only be given access to areas of the system and application that are necessary for any approved work.

12.2.3 Technical Review of Applications After Operating Platform Changes

Offis IT Operations shall review and test all new operating platform changes or updates prior to installing them in an operational environment. This will ensure that operational integrity is maintained and that the organisation’s security requirements are met by any new operating system release.

Business critical applications shall be reviewed and tested when operating platforms are changed to ensure there is no adverse impact on organisational operations or security.

12.2.4 Restrictions on Changes to Software Packages

To ensure integrity and security of vendor supplied software packages, as well as to minimise the expense and support issues associated with modified products, Offis will use standard, unmodified vendor supplied software programs whenever possible.

If modifications must be made, the organisation shall do a risk assessment to clarify and control the compromise of built-in controls and integrity processes; vendor requirements for consent; and impact of future maintenance.

Whenever possible, the organisation shall request that the vendor makes changes as part of a future standard release.

If changes must be made, an original copy of standard software shall be retained and the changes clearly documented in the operational copy.

All changes shall be thoroughly tested prior to use and clearly documented in case there is a need to reapply the changes.

12.2.5 Secure System Engineering Principles

Security shall 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.

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.

12.2.6 Secure Development Environment

Secure development environments should be established for system development and integration efforts.

Such environments shall take into consideration:

- Sensitivity of data to be processed, stored and transmitted by the system;
- Applicable external and internal requirements;
- Security controls already implemented that support system development;
- Trustworthiness of personnel working in the environment;
- Control of access to the development environment;
- The need for segregation between different development environments;
- Control over movement of data from and to the environment.

12.2.7 Outsourced Development

Where system development is outsourced, the following shall be in place:

- Licensing arrangements, code ownership and intellectual property rights related to the outsourced content;
- Contractual requirements for secure design, coding and testing practices;
- Acceptance testing for the quality and accuracy of the deliverables;
- Compliance with applicable laws.

12.2.8 System Security Testing

Testing and verification of security functionality should be carried out during development.

Independent acceptance testing should be undertaken to ensure that the system works as expected and only as expected, in proportion to the importance and nature of the system.

12.2.9 System Acceptance Testing

Systems acceptance testing of programs and related criteria shall include testing of information security requirements and adherence to secure system development practices.

Testing shall 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.

12.3 Test Data

12.3.1 Protection of Test Data

The use of operational data containing personally identifiable information or any other confidential information for testing purposes should be avoided. If personally identifiable or other confidential information is used for testing purposes, all sensitive details and content shall be protected by removal or modification.

Operational information should be erased from a test environment immediately after the testing is complete.

The copying and use of operational information should be logged to provide an audit trail.

13. Supplier Relationships

13.1 Information Security in Supplier Relationships

13.1.1 Information Security Policy for Supplier Relationships

Information security requirements for mitigating the risks associate with supplier's access to the organisation's assets should be agreed with the supplier and documented.

The types of suppliers should be identified and documented, including, but not limited to, IT services, logistics utilities, financial services, and IT infrastructure components.

The types of information access that different types of suppliers will be allowed should be identified, with the access monitored and controlled. Suppliers have applicable obligations to protect the organisation's information which should be identified and agreed upon.

Resilience, recovery and contingency arrangements are required to ensure the availability of information or information processing provided by either party in a supplier relationship.

13.1.2 Addressing Security Within Supplier Agreements

Supplier agreements should be established and documented to ensure that there is no misunderstanding between the organisation and the supplier regarding both parties' obligations to fulfil relevant information security requirements.

Terms that shall be considered for inclusion in supplier agreements include:

- Description of information to be provided or accessed and methods of providing or accessing information;
- Information classification, including any necessary mapping between the supplier and Offis' own classification schemes;
- Legal and regulatory requirements, including data protection, intellectual property rights and copyright, and how they will be met;
- Acceptable use of information;
- Authorised supplier personnel or conditions for authorisation and removal of authorisation;
- Information security policies relevant to the specific contract;
- Supplier's obligations to comply with the organisation's security requirements.

13.1.3 Information and Communication Technology Supply Chain

Agreements with suppliers should define requirements to address the information security risks associated with information and communications technology services and product supply chain.

For information and communication technology services, suppliers should be required to propagate the organisation's security requirements throughout the supply chain if suppliers subcontract for parts of the information and communication technology service provided to the organisation.

Assurance shall be obtained for delivered information and communication technology products that they are functioning as expected without an unexpected or unwanted features, and that critical components and their origin can be traced through the supply chain.

13.2 Supplier Service Delivery Management

13.2.1 Monitoring and Review of Supplier Services

Supplier services should be monitored and reviewed regularly to ensure that the information security terms and conditions of the agreements are being adhered to.

A service management relationship process between Offis and its suppliers should be established to monitor service performance levels, review service reports produced by the supplier, provide information about information security incidents and review as required, resolve and manage any identified problems, review information security aspects of the supplier's relationships with its own suppliers, and ensure that the supplier maintains sufficient service capability to ensure that agreed service continuity levels are maintained following major service failures or disasters.

13.2.2 Managing Changes to Supplier Services

Changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures and controls, should be managed. This needs to take into account of the criticality of business information, systems and processes involved and re-assessment of risks.

The following types of changes should be managed:

- Supplier agreements;
- Networks;
- User of new technologies;
- Adoption of new products or newer versions/releases;
- New development tools and environments;
- Physical location of service facilities
- Change of suppliers;
- Sub-contracting to another supplier.

14. Information Security Incident Management

14.1 Management of Information Security Incidents and Improvements

14.1.1 Responsibilities and Procedures

Offis shall establish management responsibilities to ensure that procedures are developed and communicated adequately within the organisation for the following:

- Incident response planning and preparation;
- Monitoring, detecting, analysing and reporting of information security events and incidents;
- Logging incident management activities;
- Handing of forensic evidence;
- Assessment of and decision on information security events and assessment of information security weaknesses;
- Response including those for escalation, controlled recovery from an incident and communication to internal and external parties.

Procedures shall be established to ensure that competent personnel handle issues related to information security incidents and that appropriate contact with authorities, external interest groups or forums related to information security incidents are maintained.

Reporting procedures shall be established to include the action to be undertaken in case of an information security event, and information security event reporting forms to facilitate the reporting action. There should be 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.

A formal disciplinary process shall be established for dealing with employees who commit security breaches.

14.1.2 Reporting Information Security Events

Offis will establish and educate employees on formal reporting and feedback procedures for all information security events. In this way, Offis will react to all security events as quickly as possible, and provide all employees with the information necessary to assist the organisation in doing so.

All suspected policy violations, breaches of physical security arrangements, uncontrolled system changes, software or hardware malfunctions, access violations, and other situations that might jeopardise Offis information or Offis information systems shall be immediately reported to the company information security officer. Malfunctions or other anomalous system behaviour may be an indicator of a security attack or security breach and thus should always be reported as an information security event.

If an employee learns that Offis confidential information has been lost, disclosed to unauthorised parties, or is suspected of being lost or disclosed to unauthorised parties, the employee shall immediately notify the owner of the information or the company information security officer.

Incidents may be used in on-going security awareness training to illustrate policy or procedures.

Incidents shall be reviewed for the purposes of learning how they can be avoided in the future.

14.1.3 Reporting Information Security Weaknesses

Offis requires all employees and contractors using the organisation's information systems to immediately report suspected security weaknesses in, or threats to, systems or services to management. These weaknesses should only be reported if actually discovered by the user.

Only users authorised by the company information security officer may test systems for suspected security weaknesses. Any unauthorised testing by users shall be considered misuse of the system and be subject to disciplinary measures.

14.1.4 Assessment of and Decision on Information Security Events

Information security events shall be assessed using an agreed information security event and incident classification scale to decide whether the event should be classified as an information security incident.

Results of the assessment and decision should be recorded in detail for the purpose of future reference and verification.

14.1.5 Response to Information Security Incidents

Information security incidents shall be responded to by a nominated point of contact and other relevant persons of the organisation or external parties.

Evidence should be collected as soon as possible after occurrence of the incident, with forensics analysis conducted as required. All involved response activities are to be properly logged for further analysis.

The existence of the incident or any relevant details should be communicated to other internal and external people or organisations with a need-to-know, and escalated as required.

Information security weaknesses found to be the cause or contributor to the incident shall be dealt with.

Once the incident has been successfully dealt with, it shall be formally closed and recorded.

Post-incident analysis should take place, as necessary, to identify the source of the incident.

14.1.6 Learning from Information Security Incidents

Mechanisms should be in place to enable the types, volumes and costs of information security incidents to be quantified and monitored.

The knowledge gained from the evaluation and resolution of information security incidents should be used to identify recurring or high impact incidents, and to determine new controls to reduce the likelihood or impact of such incidents in the future.

14.1.7 Collection of Evidence

The identification, collection, acquisition and preservation of information which can serve as evidence should be managed by internal procedures.

The procedures should take into account the chain of custody; safety of evidence; safety of personnel; roles and responsibilities of personnel involved; competency of personnel; documentation; and briefing.

15. Information Security Aspects of Business Continuity Management

15.1 Information Security Continuity

15.1.1 Planning Information Security Continuity

Planning for continuity of Offis' information security management is based on information security requirements remaining the same in adverse situations as compared to normal operational conditions.

Business continuity and disaster recovery planning tasks should take into account the organisation's information security requirements.

15.1.2 Implementing Information Security Continuity

Offis should ensure that 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.

Incident response responsibilities shall be assigned to appropriate personnel with the necessary authority and competence to manage an incident and maintain information security.

Documented plans, response and recovery procedures should be developed and approved, detailing how Offis will manage a disruptive event and maintain its information security to a predetermined level, based on management-approved information security continuity objectives.

15.1.3 Verify, Review and Evaluate Information Security Continuity

Offis shall verify the established and implemented information security management continuity by exercising and testing the functionality of, and knowledge/routine to operate, information security continuity processes, procedures and controls to ensure they are consistent with the organisation's objectives.

The validity and effectiveness of information security continuity measures should be reviewed when there are changes to information systems; information security processes, procedures and controls; or business continuity management and disaster recovery management processes and solutions.

15.2 Redundancies

15.2.1 Availability of Information Processing Facilities

Offis shall identify business requirements for the availability of information systems, and where availability cannot be guaranteed in accordance with those requirements 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.

16. Compliance

16.1 Compliance with Legal and Contractual Requirements

16.1.1 Identification of Applicable Legislation and Contractual Requirements

To avoid any legal or security breaches, Offis will define, document, and comply with all relevant statutory, regulatory, and contractual requirements for each information system and the organisation.

Each system owner shall implement controls to comply with all relevant statutory, regulatory and contractual requirements for their information system. System owners shall seek the advice of the company secretary or legal advisors for all relevant legal and security information.

Managers should identify all legislation applicable to the organisation, including compliance in different locations where business is conducted.

16.1.2 Intellectual Property Rights

All users at Offis will comply with the legal aspects of intellectual property protection and the rights and limitations of license agreements associated with proprietary software products.

The purpose of the policy is to ensure that users are aware of and comply with such restrictions as copyrights, trademarks, and design rights. Users are responsible for not violating applicable copyright, intellectual property, or other licensing rights of electronic media or software that is not the property of Offis. Furthermore, users are responsible for not using Offis intellectual property outside the limits of Offis policy or licensing.

Failure to abide by these policies will subject the user to disciplinary actions up to, and including, termination or criminal/civil charges.

16.1.2.1 Intellectual Property Standards and Training

Intellectual property rights protection shall be included in all security awareness training.

Users should be educated on:

- maintaining appropriate asset registries;
- maintaining proof of ownership or licenses;
- implementing controls to restrict the number of users to the licensed amount;
- implementing controls and checks to ensure that only licensed software is installed;
- policies and controls to assure that license conditions are met;
- policies and controls for disposing or transferring software to others;
- use of appropriate audit tools.

16.1.2.2 Software from Outside Sources

Users will not acquire or install any third party illegal software on Offis systems. Software shall only be acquired through known and reputable sources to ensure that copyright is not violated.

Users will not download or install any non-approved software from the Internet. The company information security officer will approve specific software for use from the Internet if there is a business need.

16.1.2.3 Copyrighted Material

Offis respects the copyrights of those involved in creating and distributing copyrighted material. It is the policy of Offis to fully comply with all copyright laws.

Offis provides its employees access to computer systems and the Internet to allow them to do their jobs on behalf of Offis. Employees may make occasionally use of the company's computer systems and network for personal use, where permitted.

When Offis employees need to use copyrighted materials to do their jobs, Offis acquires appropriate licenses.

Offis employees may not:

- Store of otherwise make unauthorised copies of copyrighted material on or using Offis computer systems, networks or storage media;
- Download, upload, transmit, make available or otherwise distribute copyrighted material using Offis' computer systems, networks or storage media without authorisation;
- Use or operate any unlicensed peer-to-peer file transfer service using Offis' computer systems or networks or take other actions likely to promote or lead to copyright infringement.

Offis reserves the right to:

- Monitor its computer systems, networks and storage media for compliance with this and other company policies at any time, without notice and with or without cause; and
- Delete from its computer systems and storage media, or restrict access to, any unauthorised copies of copyrighted materials it may find, at any time and with or without notice.

16.1.3 Protection of Records

Offis will protect organisational records from loss, destruction, falsification, unauthorised access and unauthorised release, in accordance with legislatory, regulatory, contractual and business requirements.

Records shall be protected according to their corresponding classification, based on the organisation's classification scheme. They should be categorised into record types, each with details of retention periods and type of allowable storage media. 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.

Storage and handling procedures for media used to store records should be implemented in accordance with manufacturer's recommendations.

Where electronic storage media are chosen, procedures to ensure the ability to access data throughout the retention period should be established to safeguard against loss due to future technology change.

16.1.4 Privacy and Protection of Personally Identifiable Information

Offis will comply with all applicable laws and regulations regarding the protection of personal data. This will ensure that Offis is collecting personal information (information that can be used to identify living individuals) in a manner that complies with laws as well as processing and disseminating that data in a lawful manner.

The appointment of a person responsible, such as an information protection officer, shall document policies and procedures that comply applicable laws and regulations for the handling of personal information for each such instance.

Information owners shall inform the appropriate information protection officer about proposals to keep information in a structured file. The information protection officer should advise information owners on policies and procedures concerning their protection and storage of such data.

Confidential information entrusted to Offis by members, business partners, suppliers, and other third parties shall be protected in accordance with Offis' security policies and shall be protected with at least the same care as Offis' confidential information.

16.1.5 Regulation of Cryptographic Controls

Cryptographic solutions are governed by various laws and regulations. Offis will comply with all applicable agreements, laws, regulations or other instruments that control the use or access of cryptographic controls.

The following restrictions on the use of cryptographic controls are applicable:

- Import and export restrictions on cryptographic software or hardware;
- Import and export restrictions on software or hardware that can have cryptographic functions added to it;
- Mandatory or discretionary methods of access by the countries' authorities to information encrypted by hardware or software to provide confidentiality of content;
- National laws.

16.2 Information Security Reviews

16.2.1 Compliance with Security Policies and Standards

To maintain the security of the organisation's information processing assets, Offis will continually monitor the organisation's compliance with its security policies and standards.

Managers shall continually monitor and review, within their area of responsibility, their users' compliance with the organisation's security policies, procedures, standards and requirements. If any non-compliance is found, managers should identify the causes of non-compliance, evaluate the need for action, implement appropriate corrective action, and review the corrective action taken to verify its effectiveness and identify any weaknesses or deficiencies.

16.2.2 Technical Compliance Review

The company information security officer will monitor the organisation's technical compliance with its security policies and standards.

A technical specialist should be used for technical compliance checking to ensure that hardware and software security controls have successfully been implemented in operational systems.

Where available, technical reports shall be generated for subsequent interpretation by a qualified technical specialist.

Penetration testing shall be done by third party experts as necessary, with care taken that a successful penetration test does not compromise systems or exploit other vulnerabilities.

The company information security officer shall oversee all technical compliance testing.