INFORMATION TECHNOLOGY SECURITY STANDARDS

Version 2.0
December 2013

Table of Contents

1 OVERVIEW 3

2 SCOPE 4

3 STRUCTURE 5

4 ASSET MANAGEMENT 6

5 HUMAN RESOURCES SECURITY 7

6 PHYSICAL AND ENVIRONMENTAL SECURITY 8

7 COMMUNICATIONS AND OPERATIONS MANAGEMENT 10

8 ACCESS CONTROL 14

9 INFORMATION SYSTEMS ACQUISITION, DEVELOPMENT AND MAINTENANCE 16

10 INFORMATION SECURITY INCIDENT MANAGEMENT 18

11 BUSINESS CONTINUITY MANAGEMENT 19

12 COMPLIANCE 20

1 Overview

1.1 The IT Security Standards

The IT Security Standards ('Standard') has been developed to underpin the IT Security Policy ('Policy') and provide consistent standards to support information security risk management across the University of Technology, Sydney ('UTS').

1.2 Purpose

Maintaining the confidentiality, integrity and availability of UTS information, including student information, whether they are in electronic or physical form is essential for UTS to maintain its reputation and position in the market as a trusted and respected University.

This Standard is based on the "ISO/IEC 27002:2006 – Information Technology – Security Techniques - Code of Practice for Information Security Management" and establishes the minimum requirements for effectively managing information security across UTS in a risk based manner.

The purpose of this Standard is to:

- Reduce the risk that UTS's information assets, (including student information) will be lost, corrupted, inappropriately used or disclosed.
- Provide a framework to identify, assess and manage areas of non-compliance to the Policy, Standard and associated standards with the objective of managing risks to UTS information assets across all UTS faculties and business units.
- Provide a framework for the establishment of appropriate standards, architectures, processes, procedures and standards to support the implementation of the Policy and Standard across UTS.
- Provide an approved frame of reference for staff, contractors and external parties who are responsible for designing, implementing and supporting secure information technology systems and infrastructure for UTS.
- Promote and support the adherence to appropriate legislation, regulation and industry standards, including but not limited to Privacy legislation, and the Payment Card Industry Data Security Standard.

UTS information (including student information) that can be accessed by staff, contractors and external parties must be protected from inappropriate use, modification, loss or disclosure.

Appropriate security standards and measures must be established, implemented, monitored, reviewed and improved as required to ensure that the Policy, Standard and the business objectives of UTS are met. These standards and measures are directly enforceable through this Standard.

These standards are also intended to be applied in conjunction with other UTS policies including but not limited to the IT Security Policy and the Acceptable Use of Information Technology Facilities.

It is the intent of UTS that this Standard is implemented and that appropriate security measures are in place, supported by standards, processes and procedures to ensure compliance.

2 Scope

2.1 Scope and Audience

This Standard applies to all UTS staff, as well as contractors and external parties who have access to UTS information systems and UTS information. This Standard applies to information in transit, accessed or stored in any form (physical or electronic media).

2.2 Achieving Compliance

Compliance to this Standard is mandatory for all users, systems and processes. Requests for deviations from this Standard are to be documented and managed using the approved process. Any requests for deviations from this Standard must be approved by the Chief Information Officer or their delegate.

Staff and contractors who breach this Standard may be subject to disciplinary action. A breach of this Standard may be treated as misconduct under the Acceptable Use of Information Technology Facilities.

2.3 Authority

The Chief Information Officer is authorised to approve this Standard and to require processes to monitor and ensure compliance to the Standard.

UTS has a responsibility to ensure that staff, students, contractors and external parties are aware of the requirements of the Standard and to implement appropriate measures to ensure compliance with the Standard. These measures may involve implementing changes in organisational behaviours or practices to ensure compliance with the Standard.

2.4 Roles & Responsibilities

2.4.1 Staff and Contractors

All staff and contractors, (including those of external parties) must ensure that they are aware of their responsibilities in relation to this Standard and that all requirements of this Standard are met as it relates to their role.

2.4.2 Managers

Managers (including people with direct reports, team leaders, supervisors of staff or contractors and others with people management responsibilities) must ensure that their team members are aware of and understand this Standard and that all the requirements of this Standard are met by their team members in the performance of their duties.

2.4.3 Information Asset Owners

Information asset owners must ensure that all information assets that they are accountable for are appropriately security classified, kept secure, disposed of securely and protected from compromise and misuse.

2.4.4 Business Application Owners

Business application owners must periodically (or when need dictates) have the risks formally assessed to which their business applications are exposed, and implement security controls based on the results of that risk assessment.

2.4.5 System Managers

System managers must implement and manage security controls in line with the risk and compliance requirements of the business.

2.4.6 Information Security

Information Security must ensure that appropriate 'due diligence' standards are applied in protecting UTS's proprietary, student and other confidential and personal information.

2.4.7 Manager, Governance and Compliance

The Manager, Governance and Compliance must provide information security risk management advice and assistance to the Executive, Managers, Information Asset Owners, Business Application Owners, System Managers and others as required by business needs.

3 Structure

Information Security at UTS is governed by the following.

3.1 Standards

This Standard establishes the minimum objectives for effectively protecting UTS information and information systems. It consists of high level statements that

clearly define the expectations across UTS for protecting information. The Standard defines the business and security goals, but the Standard does not mandate how these goals are implemented. The Standard is binding on all staff, contractors and external parties who develop, view, transact and maintain information and information systems.

3.2 Processes and Procedures

Processes and procedures describe the detailed steps required to perform specific tasks including the steps required when unexpected results occur. Processes and procedures are binding on all staff, contractors and external parties for whom they are applicable.

4 Asset Management

Objective: To achieve and maintain appropriate protection of assets.

4.1 Responsibility for Assets

4.1.1 Inventory of Assets

Appropriate details for hardware and software assets must be clearly identified, recorded and maintained in a centralised asset inventory.

4.1.2 Management of information Assets

Information assets must be appropriately managed based on their security classification.

4.1.3 Ownership of Assets

All information and assets associated with information processing facilities must have a designated owner within UTS.

4.1.4 Acceptable use of Assets

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

4.2 Information Security Classification

4.2.1 Classification Standards

Information must be classified in terms of its value, legal and regulatory requirements, sensitivity and criticality.

4.2.2 Information Labeling and Handling

Procedures for information labeling and handling must be developed and implemented in accordance with the security classification scheme adopted by UTS.

5 Human Resources Security

Objective: To ensure that staff, contractors and external parties understand their responsibilities for protecting UTS information and systems.

5.1 Prior to Employment

5.1.1 Roles and Responsibilities

Security roles and responsibilities of staff, contractors and external parties must be clearly explained for each user at UTS.

5.1.2 Screening

Background verification checks on candidates for employment, contractors and external parties must be conducted in accordance with relevant laws and regulations and be proportional to the classification of the information to be accessed and the perceived risks.

5.1.3 Terms and Conditions of Employment

All staff, contractors and external parties must read, understand and sign the IT Security Policy and the Acceptable Use of Information Technology Facilities which states their information security responsibilities.

5.2 During Employment

5.2.1 Manager Responsibilities

Managers must require all staff, contractors and external parties to apply security in accordance with this IT Security Policy, this Standard and associated security standards, architectures, processes and procedures.

5.2.2 Information Security Awareness, Education and Training

All staff, contractors and external parties must undertake information security awareness training at regularly defined intervals.

5.2.3 Disciplinary Process

There must be a formal and approved disciplinary process for staff who have committed a security breach.

5.3 Termination or Change of Employment

5.3.1 Termination or Change of Employment Responsibilities

Responsibilities for performing employment termination or change of employment processes must be clearly defined and assigned.

5.3.2 Return of Assets

All staff, contractors and external parties must return all UTS assets in their possession upon termination or change of their employment, contract or agreement, unless otherwise authorised.

5.3.3 Removal of Access Rights

The access rights of all staff, contractors and external parties to information and information systems must be removed immediately upon termination or change of their employment, contract or agreement.

6 Physical and Environmental Security

Objective: To prevent unauthorised physical access, damage and interference to UTS premises, systems and information assets.

6.1 Secure Areas

6.1.1 Physical Security Perimeter

Information processing facilities and information assets must be protected from unauthorised physical access, damage and interference.

6.1.2 Physical Entry Controls

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

6.1.3 Securing Offices, Rooms and Facilities

Physical security measures for offices, rooms and facilities must be designed and applied to protect information assets.

6.1.4 Protecting Against External and Environmental Threats

Physical protection against damage from fire, flood, earthquake, explosion, civil unrest and other forms of natural or man-made disaster must be designed and applied.

6.1.5 Working in Secure Areas

Physical protection and requirements for working in secure areas must be designed and applied.

6.1.6 Public Access, Delivery and Loading Areas

Physical access points such as delivery and loading areas and other points where unauthorised persons may enter UTS premises must be controlled and isolated from information processing facilities to avoid unauthorised access or interference.

6.2 Equipment Security

6.2.1 Equipment Siting and Protection

Equipment must be located and protected to reduce the risks from environmental threats, hazards and opportunities for unauthorised access.

6.2.2 Supporting Utilities

Key equipment must have appropriate controls in place to manage disruptions from power failures and other failures in supporting utilities.

6.2.3 Cabling Security

Power and telecommunications cabling services must have appropriate controls implemented to minimise the risk of interception, failures or damage.

6.2.4 Equipment Maintenance

Key equipment must be correctly maintained to ensure its continued availability, integrity and confidentiality.

6.2.5 Security of Equipment Off-Premises

Appropriate security controls must be applied to off-site equipment, taking into account the additional and different risks of working outside UTS premises.

6.2.6 Secure Disposal or Re-Use of Equipment

Prior to disposal, storage media must be checked in line with its classification to ensure that licensed software and any sensitive data has been removed or securely overwritten.

6.2.7 Removal of Property

Equipment, information and software must not be taken off-site without authorisation.

6.2.8 Risk Assessment for Premises

A security risk assessment must be performed and acted upon for any premises where UTS conducts its business or processes its information

7 Communications and Operations Management

Objective: The purpose of this Standard section is to:

- Secure the operation of information processing facilities.
- Implement and maintain the appropriate level of information security and service delivery.
- Minimise the risk of system failures.
- Protect and maintain the integrity and availability of software, information and information processing facilities.
- Ensure the protection of information in networks and the protection of the supporting infrastructure.
- Prevent unauthorised disclosure, modification, removal or destruction of assets and interruption of business activities.
- Maintain the security of information and software exchanged within UTS and with any external party.
- Ensure the security of electronic commerce services and manage their use.
- Detect unauthorised information processing activities.

7.1 Operational Procedures and Responsibilities

7.1.1 Documented Operating Procedures

Operating procedures must be documented and maintained and made available to authorised personnel.

7.1.2 Change Management

Changes to information processing facilities and information systems must be appropriately controlled.

7.1.3 Segregation of Duties

Duties and areas of responsibility must be segregated to reduce opportunities for unauthorised or unintentional modification or misuse of information assets.

7.1.4 Separation of Development, Test and Production Facilities

Separate development, test and production facilities must be in place to manage sensitive and critical information and systems.

7.2 External Party Service Delivery Management

7.2.1 Service Delivery

Security controls, service definitions, and delivery levels that are included in external party service agreements must be implemented, operated and maintained by external parties.

7.2.2 Monitoring and Review of External Party Services

Services, reports and records provided by external parties must be regularly monitored, reviewed and audited.

7.2.3 Managing Changes to External Party Services

Changes to the provision of services must be managed, taking into account the sensitivity and criticality of business systems and processes involved and re-assessment of risks.

7.3 System Planning and Acceptance

7.3.1 Capacity Management

The use of system resources must be monitored and managed and projections made of future capacity requirements for key information systems.

7.3.2 System Acceptance

Acceptance criteria for new information systems, upgrades and new versions must be established and suitable tests of the system(s) carried out during development and prior to acceptance.

The operational requirements of new information systems must be established, documented and tested prior to acceptance and implementation.

1. 10.4. Protection against Malicious and Mobile Code

7.3.3 Controls Against Malicious Code

Appropriate detective, preventative and corrective measures, in conjunction with user awareness procedures, must be implemented on information processing facilities and systems to protect against viruses and malicious code.

7.3.4 Controls Against Mobile Code

Security controls must be implemented to govern the use of mobile code and to prevent the execution of unauthorised mobile code.

7.4 Back-Up

7.4.1 Information Back-Up

Back-up copies of information and software must be taken and tested regularly in accordance with the agreed formal backup requirements.

7.5 Network Security Management

7.5.1 Network Controls

Networks must be managed and controlled to provide appropriate protection from threats and to maintain security for the systems and applications using the network, including information in transit.

7.5.2 Security of Network Services

Security features, service levels and security management requirements of all network services must be identified and included in any network service level agreement.

7.6 Media Handling

7.6.1 Management of Removable Media

Formal procedures must be implemented for the management of removable media.

7.6.2 Disposal of Media

Media must be disposed of in an approved manner, which is safe and secure.

7.6.3 Information Handling Procedures

Procedures for the handling and storage of information must be established to protect this information from unauthorised disclosure, misuse or loss.

7.6.4 Security of System Documentation

All sensitive and critical system documentation must be protected from unauthorised access.

7.7 Exchange of Information

7.7.1 Information Exchange Policies and Procedures

Exchanges of information and software between internal or external parties must be controlled based on formal exchange procedures.

Security controls and procedures must be established to protect information in transit.

7.7.2 Exchange Agreements

Exchange of information and software between UTS and external parties must be subject to a formal agreement.

Where contracts are being established between UTS and external parties, a formal security risk assessment must be conducted and identified risks appropriately managed.

7.7.3 Physical Media in Transit

Media containing information must be protected against unauthorised access, misuse or corruption during transportation beyond UTS physical boundaries.

7.7.4 Electronic Messaging

Information involved in electronic messaging must be protected in accordance with its security classification and associated risks.

7.7.5 Business Information Systems

Procedures for connection to external party information systems from UTS information systems must be developed and implemented to manage the associated information security risks.

7.8 Electronic Commerce Services

7.8.1 Electronic Commerce

Information involved in electronic commerce passing over public networks must be protected from fraudulent activity, contract dispute, unauthorised disclosure, modification or loss.

7.8.2 On-line Transactions

Information involved in on-line transactions must be appropriately protected to prevent incomplete transmission, mis-routing, unauthorised message alteration, unauthorised disclosure, unauthorised message duplication or replay.

7.8.3 Publicly Available Information

The integrity of information made available on publicly accessible UTS systems must be protected to prevent unauthorised modification.

7.9 Monitoring

7.9.1 Audit Logging

Audit logs recording user activity, exceptions and information security events on key information systems must be produced, maintained and retained for an agreed period in accordance with legal, regulatory and operational requirements.

7.9.2 Monitoring System Use

A formal security risk assessment must be conducted to determine the systems to be monitored.

Information processing facilities must be appropriately managed and monitored.

7.9.3 Protection of Log Information

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

7.9.4 Administrator and Operator Logs

All system administrator and system operator activities must be logged.

7.9.5 Fault Logging

Faults of key information systems must be logged and analysed and the appropriate action taken.

7.9.6 Clock Synchronisation

The clocks of all relevant information processing systems within UTS must be synchronised with an agreed accurate time source.

7.9.7 Information Security Testing

The security controls of information systems must be formally and periodically tested based on risk.

8 Access Control

Objective: To control access to information and information systems.

8.1 Business Requirements for Access Control

8.1.1 Access Control

Access to UTS information and information systems must be controlled in accordance with the relevant security standards, architectures, processes and procedures, and be subject to the principles of least privilege and segregation of duty.

8.2 User Access Management

8.2.1 User Registration

A formal user registration and de-registration procedure must be in place for granting and revoking access to all information systems and services.

8.2.2 Privilege Management

Formal procedures must be in place to control the allocation of access rights to information systems and services.

The allocation and use of privileges must be restricted and controlled.

8.2.3 User Password Management

Allocation of passwords must be controlled through an approved security management process.

8.2.4 Review of User Access Rights

Business units must review user access rights for key systems at regular intervals using an approved process.

8.3 User Responsibilities

8.3.1 Password Use

Users must be made aware of their responsibilities regarding the selection and use of passwords.

8.3.2 Unattended User Equipment

Users must ensure that unattended equipment is appropriately protected and secured.

8.3.3 Clear Desk and Clear Screen Standard

A clear desk Standard for papers and removable storage media and a clear screen Standard for information processing facilities must be adopted to manage risks to sensitive and critical information.

8.4 Network Access Control

8.4.1 Standard on Use of Network Services

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

8.4.2 User Authentication for External Connections

Appropriate authentication methods must be used to control remote access to UTS information systems.

8.4.3 Equipment Identification in Networks

Appropriate controls must be in place to manage unauthorised equipment when connecting to the UTS network.

8.4.4 Remote Diagnostic and Configuration Port Protection

Physical and logical access to diagnostic and configuration ports must be appropriately controlled.

8.4.5 Segregation in Networks

Appropriate security controls must be in place to segregate UTS networks in accordance with the relevant security standards and security architecture.

8.4.6 Network Connection Control

Network access from external parties to any UTS network must be restricted to only allow access to perform the agreed services.

8.4.7 Network Routing Control

Routing controls must be implemented for networks to ensure that computer connections and information flows do not breach the access control requirements of business applications, infrastructure and networks.

8.5 Operating System Access Control

8.5.1 Secure Log-On Procedures

Access to operating systems must be controlled by a secure log-on procedure.

8.5.2 User Identification and Authentication

All users must be assigned a unique identifier to access information systems, for their personal use only.

A suitable authentication technique must be implemented to substantiate the claimed identity of all users.

8.5.3 Password Management System

Systems for managing passwords must ensure that passwords are managed in accordance with the applicable security standards.

8.5.4 Use of System Utilities

The use of utility programs capable of overriding system and application controls must be restricted and secured appropriately.

8.5.5 Session Time-Out

User sessions must be forced to time out after a defined period of inactivity.

8.5.6 Limitation of Connection Time

Restrictions on connection times must be used to provide appropriate security for key applications.

8.6 Application and Information Access Control

8.6.1 Information Access Restriction

Access to information and application system functions by users and support personnel must be restricted in accordance with the relevant standards.

8.6.2 Sensitive System Isolation

Sensitive information systems must have a dedicated (isolated) computing environment based on risk.

8.7 Mobile Computing and Teleworking

8.7.1 Mobile Computing and Communications

Appropriate security controls must be adopted to protect against the risks of using mobile computing and communication facilities.

8.7.2 Remote Access

Appropriate security controls must be implemented to manage remote access activities.

9 Information Systems Acquisition, Development and Maintenance

Objective: To ensure that security is an integral part of information systems.

9.1 Security Requirements of Information Systems

9.1.1 Security Requirements Analysis and Specification

Statements of business requirements for new information systems (or enhancement to existing information systems) must specify the requirements of security controls prior to their design, development and implementation.

9.2 Correct Processing in Applications

9.2.1 Input Data Validation

Data input to applications must be validated to ensure that the data is correct and appropriate.

9.2.2 Control of Internal Processing

Validation checks must be incorporated into applications to detect any corruption of information through processing errors or deliberate acts.

9.2.3 Message Integrity

Requirements for ensuring authenticity and protecting message integrity in applications must be identified and appropriate controls identified and implemented.

9.2.4 Output Data Validation

Data output from applications must be validated to ensure that the processing of stored information is correct and appropriate to the circumstances.

9.3 Cryptographic Controls

9.3.1 Standard on the Use of Cryptographic Controls

Cryptographic controls must only be used in accordance with relevant standards.

All information assets classified as Confidential must be appropriately protected by cryptographic controls.

9.3.2 Key Management

Cryptographic key management must be in place to support UTS use of cryptographic techniques.

9.4 Security of System Files

9.4.1 Control of Operational Software

Security controls must be in place to prevent the installation of inappropriate or unauthorised software on all information systems.

9.4.2 Protection of System Test Data

Data masking procedures must be employed when using sensitive data outside of the production environment or any environment without controls equivalent to the related production environment.

9.4.3 Access Control to Program Source Code

Access to program source code must be restricted and appropriately controlled.

9.5 Security in Development Processes and Support Processes

9.5.1 Change Control Procedures

The implementation of changes must be controlled by the use of approved change control procedures.

9.5.2 Technical Review of Applications After Operating System Changes

When operating systems are changed, key applications must be appropriately tested to ensure there is no adverse impact on organisational operations or security.

9.5.3 Restrictions on Changes to Software Packages

Risks associated with the modification of vendor supplied software packages must be appropriately controlled and authorised.

9.5.4 Information Leakage

Security controls must be in place to manage the risks associated with sensitive information leakage.

9.5.5 Outsourced Software Development

All outsourced software development must be supervised, monitored and be performed using approved security standards.

9.6 Technical Vulnerability Management

9.6.1 Control of Technical Vulnerabilities

Information systems connected to the UTS network must be assessed for vulnerabilities.

Vulnerabilities must be remediated based on risk and in a timely manner.

10 Information Security Incident Management

Objective: To ensure information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken.

10.1 Reporting Information Security Events and Weaknesses

10.1.1 Reporting Information Security Events

Procedures must be in place to identify, manage and report information security incidents in a timely manner.

10.1.2 Reporting Security Weaknesses

All staff, contractors and external parties of information systems and services must note and report any observed or suspected security weaknesses in those systems or services, to the ITD Help Desk.

10.2 Management of Information Security Incidents and Improvements

10.2.1 Responsibilities and Procedures

Management responsibilities and procedures must be established to ensure a timely, effective and orderly response to information security incidents.

10.2.2 Learning from Information Security Incidents

A process must be in place to quantify and monitor information security incidents to identify recurring or high impact incidents.

10.2.3 Collection of Evidence

For information security incidents involving potential legal action, evidence must be collected, handled, retained and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s).

11 Business Continuity Management

Objective: The purpose of this Standard area is to:

- Provide direction to counteract interruptions to business activities.
- Protect critical business processes from the effects of major failures of information systems or disasters.
- Ensure their timely resumption.

11.1 Information Security Aspects of Business Continuity Management

11.1.1 Including Information Security in the Business Continuity Management Process

Business continuity and disaster recovery processes must address information security and risk requirements.

11.1.2 Business Continuity and Risk Assessment

Risks that can cause interruption to business processes must be identified, assessed and managed.

11.1.3 Developing and Implementing Continuity Plans Including Information Security

Business continuity and disaster recovery plans must maintain or restore operations and ensure availability of information at the required level following interruption or failure of critical business processes.

11.1.4 Business Continuity Planning Framework

A single framework of business continuity and disaster recovery must be maintained to ensure it consistently addresses information security requirements and to identify priorities for testing and maintenance.

11.1.5 Testing, Maintaining and Re-Assessing Business Continuity Plans

Business continuity and disaster recovery plans must be tested and updated regularly to ensure that they are up to date and effective.

12 Compliance

Objective: To avoid breaches of any law, statutory, regulatory or contractual obligations and of any security requirement.

12.1 Compliance with Legal Requirements

12.1.1 Identification of Applicable Legislation

All relevant legal, statutory, regulatory and contractual requirements and UTS' approach to meet these requirements must be explicitly defined, documented and kept up to date for each information system.

12.1.2 Intellectual Property Rights (IPR)

Appropriate procedures must be implemented to ensure compliance with legislative, regulatory and contractual requirements on the use of material in respect of which there may be intellectual property rights and on the use of proprietary software products.

12.1.3 Protection of Organisational Records

Important records must be protected from loss, destruction and falsification in accordance with legal, statutory, regulatory, contractual and business requirements.

12.1.4 Data Protection and Privacy of Personal Information

Information and privacy must be protected as required by relevant legislation, regulations and applicable contractual agreements.

12.1.5 Prevention of Misuse of Information Processing Facilities

Users must use information processing facilities in accordance with the Acceptable Use of Information Technology Facilities and not use the information processing facilities for unauthorised purposes.

12.1.6 Regulation of Cryptographic Controls

Cryptographic controls must be used in compliance with all relevant laws, regulations and agreements.

12.2 Compliance with the IT Security Policy, IT Security Standards, Standards and Security Architecture

12.2.1 Compliance with the IT Security Policy, IT Security Standards, Standards and Security Architecture

Business units must ensure that processes and procedures are carried out correctly to achieve compliance with the IT Security Policy, this Standard and its supporting standards and architectures.

12.2.2 Technical Compliance Checking

Information systems must be regularly checked for compliance with appropriate security standards.

12.2.3 Deviations

Deviations from this Standard and supporting standards, architectures, processes and procedures must be approved by the Chief Information Officer for all information and systems unable to meet the requirements of this Standard.

12.3 Information Systems Audit Considerations

12.3.1 Information Systems Audit Controls

Audit requirements and activities involving checks on operational systems must be carefully planned and agreed to minimise the risk of disruptions to business processes.

12.3.2 Protection of Information Systems Audit Tools

Access to information systems audit tools must be protected to prevent possible misuse or compromise.