NUS
IT SECURITY POLICY

Version 3.9

1 Jun 2021

Table of Contents

Chapter 1 NUS IT Security Policy: Introduction to Information Technology (IT) Security Policy

1 Purpose and scope

The purpose of this Policy is to define the minimum security measures required for the protection of information systems as well as the information contained and processed by the systems. These controls are described throughout the remaining sections of the Policy.

2 Introduction

Information in IT Systems is an asset which, like other important business assets, has value and consequently needs to be suitably protected. Information security protects information from a wide range of threats in order to ensure operations continuity and minimize business damage and maximize return on IT investments.

The National University of Singapore (NUS) information systems landscape comprises of a broad range of information systems from personal Internet/Intranet web servers to highly sensitive and critical corporate systems. The systems have different characteristics in the following key areas:

- Sensitivity of information
- Criticality to operations of the University, Departments and Faculties
- Risk exposure
- Potential impact to NUS in the event of a security breach

The implementation and management of the security of this diverse range of systems, with varying security requirements, throughout the entire system life cycle, will be addressed by the NUS IT Security Policy.

The Policy defines security measures so that NUS information assets are protected and consistency in the implementation and practice of security throughout NUS.

3 Information Security

3.1 Deviations from IT Security Policy

3.1.1 Deviations from the IT Security Policy may be necessary based on operational, technical and/or cost considerations.

When a need arises that dictates that an exception to the Policy is in the best interests of NUS:

- A deviation approval request should be submitted to Chief Information Technology Officer (CITO), NUS IT;
- The request must include justifications based on a risk assessment process so that management is aware of the risks to NUS. The justifications should include the following information:
  - Security measure that has to be deviated from;
  - Reasons for the deviation;
  - Alternative security measures that have been implemented;
  - Potential impact to NUS should a breach in security occur; and

- The period for which this deviation is required for.

3.2 Intended audience

3.2.1 This IT Security Policy is intended to be read by all staff and students of NUS and all other external parties that have dealings with NUS information system resources, including the use, design, audit, implementation and maintenance of these resources.

3.3 Key security objectives

3.3.1 Information security is characterized here as the preservation of three key security objectives:

- Confidentiality: ensuring that information is accessible only to authorized users;
- Integrity: safeguarding the accuracy and completeness of information and information processing systems;
- Availability: ensuring that authorised users have access to information and associated assets when required.

Increasingly, organizations and their information systems and networks are faced with security threats that attempt to compromise one or more of the above security objectives. These threats, from a wide range of sources, include computer-assisted fraud, espionage, sabotage, vandalism, fire or flood, computer viruses, computer hacking and denial of service attacks. Incidents and attacks arising from such threats have become more common and attacks have become more ambitious and increasingly sophisticated.

Information security is a process, which is achieved by implementing a suitable set of security measures, covering physical, environmental, personnel, technical and organisation structures security standards and procedures. These controls, as defined in the NUS IT Security Policy together with more detailed security procedures and guidelines, need to be established to ensure that NUS information systems and assets are adequately protected from a wide range of security threats.

3.4 Non-compliance

3.4.1 Every staff, student and external party that has dealings with NUS information system resources is responsible for protecting and preserving the information in accordance with NUS IT Security Policy

Non-compliance with NUS IT Security Policy is viewed seriously and will result in disciplinary action up to and including legal action and termination.

4 Terminology

The terminology used in this Policy to convey the level of compliance to the requirements set out is as follows: Must, Shall, or Mandatory: The item mentioned is an absolute requirement and compliance is mandatory. Should: The item mentioned indicates recommended activities.

Chapter 2 NUS IT Security Policy: Risk Analysis for Information Systems

1 Purpose and scope

The objective of risk assessment is to gain a sound understanding of the security risks associated with an information system and to determine which controls should be put in place to reduce the level of risk or to lessen the impact of a security breach.

2 Introduction

Risk assessment is an essential part of an effective approach to IT systems security. Risk assessment is performed by business owners and provides a practical mechanism for understanding the magnitude of security exposures, and assists in the evaluation and selection of appropriate controls.

3 Performing Risk Analysis

3.1 Conduct of risk analysis

3.1.1 For high impact projects, risk analysis should be performed at the initiation stage of the systems development project so that the required controls can be incorporated to the design of the system and the business processes. Risk analysis should also be performed after the system is in operation and whenever significant new developments are initiated.

3.2 Risk Analysis Process

3.2.1 A business impact analysis should be performed to assess the impact if a security breach were to occur.

Security breaches involving data or IT services, can be in the form of:

- A loss of confidentiality;
- A loss of integrity; or
- A loss of availability.

Business impact can include, but is not limited to:

- Disruptions to NUS operations;
- Legal liabilities
- Direct or indirect financial losses;
- Damage to the University's reputation and good standing; and
- Infringement of privacy issues.

3.2.2 A threat and vulnerability assessment should be performed to identify all possible risks originating from human, environmental or technical causes. Examples of threats include:

- Intentional acts – theft, fraud, information modification, hacking;
- Accidental acts – errors and omissions, information deletion/destruction, negligence;
- Natural catastrophes – fire, water damage, lightning; and
- Technical threats – bugs, viruses and malicious codes, equipment failure.

3.2.3 Where the level of controls is inadequate, System Owner together with IT professional will need to strengthen the controls. The Data Steward can choose to accept the risk.

Chapter 3 NUS IT Security Policy: IT Security Management

1 Purpose and scope

This chapter defines the various roles within NUS that are assigned responsibilities pertaining to the protection of information resources.

2 Introduction

Everyone associated with NUS has a role in information security. Due care must be exercised in the protection of IT information resources by clearly defining roles and responsibilities of management and users relating to information security.

3 Information Security Organisation

3.1 NUS IT Steering Committee

3.1.1 NUS IT Steering Committee is chaired by Provost and Deputy President and comprises of members from key departments. This committee provides high level support and commitment for NUS information security initiatives.

3.2 Information security responsibilities

3.2.1 Management of NUS IT sets strategic direction for NUS information security initiatives and provides support, commitment and resources for NUS information security initiatives.

3.2.2 Please refer to the NUS Data Management Policy for the details of the roles and responsibilities of the following:
Data Owner
Data Stewards
Data Managers
System Owners
Data Users
Data Administrators
Database Administrators
Application Developers
IT Security Group

3.2.3 All systems shall be owned by the respective business/operating units and not by the IT Department.

3.2.4 Systems and network administrators are personnel designated to maintain, operate and implement technology solutions for NUS.

Systems and network administrators are responsible for deploying and implementing security controls on an operational basis.

The systems and network administrators’ responsibilities include, but are not limited to:

- User account administration;
- Application of system and network security patches;

- System and network documentation;
- Monitoring system and network performance; and
- Application of necessary technical security controls.

Additional security related responsibilities include, but are not limited to:

- Subscribe to relevant security advisories;
- Resolve vulnerabilities detected by security scans conducted by IT Security;
- Communicate to the IT Security Group on security-related incidents and issues;
- Assist in the investigation of security breaches/incidents;
- Review security related and access logs in accordance with the approved log review procedures; and
- Comply with the security standards, procedures and guidelines.

3.3 Review of information security

3.3.1 NUS IT Security Policy must be reviewed every twelve (12) months and whenever there are changes in the security strategies in NUS.

3.3.2 Issues arising from reviews must be resolved and recommendations implemented and incorporated into NUS IT Security Policy, where applicable.

3.4 Review of Functional SOPs and documentations

3.4.1 All Standard Operating Procedures (SOPs), procedures, guidelines and documentations, etc shall be reviewed every twelve (12) months and whenever there are major changes in the scope of work.

3.5 Third party access

3.5.1 Where there is a business need for third party connection, a risk assessment must be carried out by the requesting department and NUS IT to determine security implications and control requirements.

3.5.2 All non-NUS personnel that require access to NUS information resources must have a NUS employee sponsor. The sponsor will be held responsible for all actions taken by the sponsored.

3.5.3 Each third party employee, contract personnel, consultant, or contractor working directly for NUS either onsite or offsite who need to access sensitive data must sign a Non-Disclosure Agreement (NDA).

3.5.4 NUS must, at minimum, subject third party service providers to the same physical and logical access restrictions to which an internal user would be subjected. In addition, access to information must be limited to what is required to complete the work. Exceptions should be approved by the Chief Information Technology Officer (CITO), NUS IT.

3.5.5 All network connections to external entities must be protected by firewall(s).

3.6 Supplier Management

3.6.1 Supplier refers to Vendors, Contractors, Auditors, partners or other external parties supplying IT product or service to NUS.

3.6.2 Where Supplier proposed Cloud solutions, user shall reference NUS Cloud Policy to perform risk assessment and make informed decisions on adoption of Cloud.

3.6.3 Where access is required by Supplier to University Data and IT Resources, Supplier is required to sign NDA and comply with AUP, IT Security Policy, Data Management Policy and Guideline on Use, Classification and Protection of University Data where applicable.

3.6.4 Agreement with Supplier may include the following requirements:

(a) Compliance obligations

(i) Regulatory

(ii) Contractual

(b) Service level agreement (e.g. Availability, Response time)

(c) Logical/physical access management

(d) Right to monitor and review (e.g. privilege accounts, accesses, system performance, logs, configurations, transactions)

(e) Right to audit (including sub-contractor)

(f) Information classification

(g) Information processing (e.g. check for validity, accuracy, integrity, authenticity)

(h) Information handling (e.g. protection of information store, transfer and dispose),

(i) Backup, incidents, contingency and disaster recovery management

3.7 Changes to Supplier Agreement should take into account the changes of IT security policy, audit recommendations, risk assessment, incidents response.

Chapter 4 NUS IT Security Policy: Access Control Security

1 Purpose and scope

This chapter defines the control requirements for access to NUS information system resources.

2 Introduction

Allowing unnecessary access to NUS information system resources also invites unnecessary risk of confidentiality and integrity problems occurring due to accidental or intentional acts. Therefore, access to all information resources must be granted in a controlled manner driven by business requirements. The overall guideline is that access must only be granted based on need-to-have basis.

3 Business requirements for access control

3.1 Access control standards

3.1.1 Data Users must obtain permission from the Data Manager and demonstrate a justifiable business case to access the data. Data Managers should grant access on a need-to-know basis as required by job functions and in accordance to applicable laws and/or regulatory restrictions. Unnecessary access to system or data leads to unnecessary risks; therefore, a minimal approach must be taken when assigning access.

3.1.2 User access must be profiled using roles based upon job description, duties or function. The use of roles assists in the management of user access and provides consistency in the assignment of rights.

3.1.3 The rules used in the assignment of rights based on user roles must be explicit and rights assigned must be adequately segregated such that no single user has the ability to commit fraudulent or malicious activities. Access rights granted to each role should be documented and communicated to users and all relevant staff responsible for user access administration.

3.1.4 The access to information must be removed as soon as access is no longer needed.

4 User access management

4.1 Account and password management

4.1.1 Each system user-ID must be unique and associated with only one user to whom it has been assigned.

4.1.2 Common privileged accounts should only be used by authorized personnel for administrative purposes only. For users with similar duties, group or role based access controls should be used to assign permissions and accesses to individual accounts.

4.1.3 Account administrators must consistently use NUS approved user-ID naming standards.

4.1.4 Where technically feasible, systems and applications should be configured to only accept passwords that are of a minimum of eight (8) characters in length and be comprised of letters, numbers, and/or special characters.

4.1.5 Initial issued passwords must not be easily associated with NUS or the user (i.e. NRIC number, employee number, address, numerical equivalent of name, etc.) and should have a minimum length of eight (8) characters.

4.1.6 Where technically feasible, systems and applications must use password history techniques to maintain a history of used passwords. This feature will prevent users from reusing passwords when they change their passwords. The history file must contain, at the least, the last six (6) user passwords and store them in encrypted form.

4.2 Authentication schemes

4.2.1 Access to NUS classified information resources should, at minimum, require a user to supply a unique user-ID and a secret password for authentication.

4.2.2 A strong authentication mechanism should be implemented for sensitive systems. This includes the use of LDAP and RADIUS, etc.

4.2.3 Authentication methods may require one or more of the following: something you have e.g., a token-based card, something that you know e.g., as a password, and something you are e.g., a thumbprint.

Advanced authentication schemes such as two-factor authentication, is recommended to be deployed for accesses to NUS critical or sensitive information resources. In such a case, users must possess two of the three requirements for authentication.

4.3 Privileges and rights management

4.3.1 Authorisation for privileged application or system level (e.g. administration accounts for operating systems, databases or applications or accounts that can override system or application controls) access must be obtained from relevant management staff responsible for the IT platform of system, prior to access being given. These privileges must be based on functional or job necessity and must only be allocated on a need-to-have basis. If it is mutually agreed that the Data Manager approval is to be obtained in place of that of the management staff responsible for the IT platform or system, it should be documented accordingly.

4.3.2 All users that have access to privileged accounts for administration or other special purposes must have their own personal accounts for normal business use. System administrators and employees given privileged accounts should not use their privileged accounts to conduct normal business activities.

4.3.3 If default or existing features are inadequate, technical solutions must be sought to prevent unnecessary or excessive privileged access.

4.3.4 A procedure to remove access to a system as soon as that access is no longer needed must be established.

4.3.5 In situations where user with access to sensitive information is terminated, the employee's immediate supervisor must ensure timely removal of the user's access rights.

4.3.6 For both terminated or suspended accounts, all sensitive accesses including access to corporate data should be denied (e.g. via deletion of accounts) and all role-based passwords known to the employee should also be changed.

4.4 Review of user access rights

4.4.1 All special or privileged access to systems (such as administrative or supervisor accounts at the application or system level) must be reviewed every twelve (12) months or when major changes are made to the IT systems.

4.4.2 The review of user access rights should be conducted every twelve (12) months to revoke rights that are no longer required by users.

4.4.3 User access rights for all NUS applications must be onboarded and managed by the central Identity and Access Management (IAM) System.

4.5 User registration

4.5.1 Users shall read and sign NUS Acceptable Use Policy before issued with any system or application access.

4.5.2 User registration procedures must include:

- Authorisation from System Owners to gain access to systems or information resources;
- Users' endorsement and acceptance of NUS acceptable use policy;
- Users' acknowledgement for receipt of account and password information; and
- Maintaining a record of all user registration history.

5 User responsibilities

5.1 Accounts and passwords

5.1.1 Users should adhere to good practices in the selection and use of passwords. Dictionary words and passwords that can be easily associated with himself or herself should be avoided.

5.1.2 Users should not reveal their passwords or share the use of their accounts with anyone.

5.1.3 NUS reserves the right to hold the user liable for damages caused by the user's failure to protect the confidentiality of his/her password.

5.2 Equipment

5.2.1 Users should ensure that NUS IT equipment issued to them for their use is not left unattended.

5.2.2 Unattended equipment should be secured appropriately with cable locks or physical access controls.

5.3 Mobile Devices

5.3.1 Users should comply to NUS Mobile Devices Security Policy when using Mobile Devices for accessing University IT resources.

6 Network access control

6.1 External network connectivity

6.1.1 External network connections must be approved by the Network Group. Firewalls should be deployed to control access to NUS network.

6.1.2 Where possible, NUS internal network-addressing scheme should be non-visible to the external network through the use of Address Translation mechanisms. This keeps external parties from easily gaining information about the structure of the network.

6.1.3 Firewalls and routers should not accept external connections that appear to be coming from internal addresses by enabling anti-spoofing mechanisms.

6.1.4 For non-permanent network circuits such as ISDN, a mechanism should be in place to disconnect connections which remain idle for more than a specific duration.

6.2 General standards

6.2.1 Network services on systems should be disabled unless a specific business reason for the service is needed and documented. Risks associated with the network service must be determined and resolved prior to implementation of the service.

6.2.2 Servers with protocols which allow packet forwarding or re-routing, must be configured to disallow this function. For example, 'IP forwarding' feature should be disabled.

6.3 Remote access

6.3.1 All remote accesses to NUS information systems must be authenticated before being permitted.

6.3.2 Two-factor authentication should be enforced for remote access to sensitive systems.

6.3.3 If remote access to administrative diagnostic ports is required, the relevant management staff responsible for the IT platform or system must assess such access to ensure only authorized personnel have access and all actions on such ports are logged.

6.3.4 VPN should be used for connection to the NUS Intranet systems from remote locations (off University premise), where applicable.

6.4 Segregation in networks

6.4.1 Full and unrestricted connection of one network segment to another segment of different sensitivity should not be allowed. Separation of network segments of different sensitivity, such as using firewalls, vlans or other means, must be implemented to increase the level of security provided during information transport/storage.

7 Operating system access controls

7.1 General standards

7.1.1 All users must have a unique user-ID. Each user account must have an associated password known only to the assigned owner.

7.1.2 For systems that have single administrative accounts, such as Unix, users with access to the administrative account must first use their normal account to log into systems before switching to the privileged administrative account. This is to identify and log the user of the administrative accounts.

7.1.3 Users given command line access to systems must, where feasible, be limited to the access or service needed via the use of restricted shells, application menu restrictions or other means.

7.1.4 For more stringent security environments, unique device identifiers using IP addresses, host names or shared secret keys should be used to limit access to specific terminals.

7.2 Superuser/administrator (emergency) ID and password management

7.2.1 Superuser/administrator accounts should not be used for daily operations and should be kept secure until required for emergency use. Operators should be provided with accounts with reduced privileges for their daily operational activities whenever the system permits.

7.3 System inactivity

7.3.1 Staff issued computers, notebooks/laptops and servers should be installed with screen-saver configured with password protection. It should activate automatically after an idle period of fifteen (15) minutes.

7.3.2 Network idle sessions must be configured to automatically timeout where technical feasible, the duration of which should depend on business requirements.

7.4 System logon standards

7.4.1 Where technically possible, a pre-login banner with appropriate warnings on unauthorised access and use should be presented to all users. This provides users a chance to terminate the login before accessing information resources that they are not authorised. This also provides NUS with legal grounds to prosecute unauthorised access. An example would be:

Property of NUS and for authorised Users only. By continuing to use this system/application which is governed by the NUS Acceptable Use Policy, you represent that you are an authorized user.

7.4.2 The content of pre-login banners should include warnings for the following:

- That the system is to be used only by authorised users and legal action will be taken against unauthorised access;
- That by continuing to use the system, the user represents that he/she is an authorised user; and
- That use of this system constitutes consent to monitoring.

7.4.3 Information of NUS network, location, or host should not be displayed at any point during the login process.

7.4.4 Systems should not provide information on the cause of unsuccessful logins. This includes identifying which portion of login credentials (user-ID or password) was incorrect.

7.5 Use of system utilities

7.5.1 A number of utilities are available to enable system administrators to perform low-level maintenance tasks on a system. If inappropriate access is gained to these utilities they may be used to circumvent logical security controls. Where technically feasible, all utilities should

- Be removed or disabled if not required;
- Be stored off-line if not required on a daily basis;
- Be restricted at the server console. If remote access is permitted, access should be restricted to authorised terminals based on IP address, shared secrets or other appropriate methods;
- Have encrypted channels for remote access so that passwords and data transmitted are protected;
- Have access restricted to a limited group of authorised users; and
- Include logging facilities to record their use.

8 Application access controls

8.1 Information access restriction

8.1.1 All users must only be provided with the minimum level of access required to perform their duties. This should be achieved using a combination of:

- Logical security within an application;
- Hiding the availability of unauthorised options;
- Restricting knowledge of application content and functionality;
- Limiting file permissions, e.g. read-only; and
- Controlling output distribution.

8.2 Sensitive system isolation

8.2.1 Sensitive applications should be segregated from other networks or systems holding less critical data by the appropriate use of firewalls.

9 Monitoring system access and use

9.1 Audit logging

9.1.1 Systems handling sensitive, valuable, or critical information must log all security-relevant events where technically feasible. Examples of security-relevant events include:

- Users switching user-ids;
- Attempts to use privileges that have not been authorised;
- Modifications to production application or system software;
- Modifications to user privileges;
- Modifications to logging subsystems;
- Successful login attempts; and
- Unsuccessful login attempts; and
- Unsuccessful attempts to access system files.

9.1.2 Logs containing computer or communications system security-relevant events must be retained for at least six (6) months. During this period, logs must be secured such that they cannot be modified, and can be read only by authorised persons. These logs are important for error correction, security breach recovery, investigations, and related efforts.

All potential security incidents must be reported immediately and handled as per NUS incident management procedure.

9.1.3 Logs help in troubleshooting and detecting security breaches and intrusions. However, large volume of logs may hinder the detection of real security problems and affect system performance.

Where system performance is affected by overheads in audit logging, an assessment should be conducted by the respective System Owner and IT professional to decide on the balance between the level of logging and system performance.

9.2 Clock synchronisation

9.2.1 System clocks should be synchronised to an agreed standard to ensure the accuracy of time stamps in audit logs. Synchronisation can be based on Greenwich Mean Time or local time and should be checked periodically so that any 'drift' can be corrected in a timely manner.

9.3 General responsibilities

9.3.1 System administrators must perform system monitoring activities as part of their daily work routine. This includes, but is not limited to, monitoring system usage and performance, user access, audit logs and system services.

9.4 Monitoring access and use

9.4.1 Procedures for monitoring application and system accesses and usage should be established. These procedures should address the following:

- Defining the roles and responsibilities of the various administrators;
- Use and access control of monitoring and alerting tools;
- Configuration of audit logs;
- Review of audit logs; and
- Supervision of monitoring activities.

9.4.2 Where technically possible, a log-monitoring tool should be used to collect and monitor all logs so as to alleviate resources required for manual log review. The tools should be capable of generating alerts when abnormal activities are detected.

Chapter 5 NUS IT Security Policy: Personnel Security

1 Purpose and scope

This chapter defines the security standards that must be applied with regards to personnel.

2 Introduction

Employees are one of the most valuable assets in any organisation. Where personnel security is concerned, safeguards should be implemented to minimise the risk of accidental or intentional acts or risks due to a lack of knowledge of good security practices.

3 Security in job definitions and responsibilities

3.1 Confidentiality agreement

3.1.1 All staff working must have a confidentiality clause in their employment letter.

3.2 Job responsibilities

3.2.1 All staff should comply with NUS Acceptable Use Policy (AUP) for IT Resources.

3.3 Personnel screening

3.3.1 The Office of Human Resources or the department should perform a background check of all staff before the staff joins NUS. This may include character references, education verification, credit check (if applicable) and independent identity check. If the employee is being hired via a third party or recruitment agency, proper screening checks must be verified by that agency as well as Office of Human Resources.

4 User exit/movements/training

4.1 Exit and movements

4.1.1 The Office of Human Resources must ensure timely updating of the staff database arising from personnel movement (including assumption, resignation, transfer, etc) so that the necessary changes to access privileges can be made on a timely basis.

4.1.2 Upon termination or transfer, the system administrators must ensure that the user's ID access is revoked or modified. Any items issued to the employee or vendor such as notebooks/laptops, keys, ID cards, software, data, documentation, manuals etc. must be returned to their supervisor.

4.1.3 The students' ID access must be disabled when the student has left the university.

4.2 Security training and awareness

4.2.1 All new staff and students should have access to copies of all relevant IT Security Policy, security standards, procedures and security awareness materials appropriate for their position and role in NUS. The material is made available via the University intranet.

4.2.2 Users should familiarise themselves with NUS IT Security Policy and all other relevant security standards and procedures. Ignorance will not be accepted as a valid reason for non-compliance.

4.2.3 It is the responsibility of NUS IT Security Group to promote constant security awareness to all users.

4.2.4 Security advisories should be posted to ensure that all users who may be affected have access to these documents. Several options are available for posting security advisories; including, e-mail and/or MOTD. Security advisories should include warnings on specific risks including issues such as viruses, social engineering, technical vulnerabilities and NUS-specific risks and countermeasures.

Chapter 6 NUS IT Security Policy: Physical and Environmental Security

1 Purpose and scope

This chapter defines the physical security and environmental standards for computer facilities and the information assets located therein. It establishes standards that must be followed in order to obtain a minimum level of physical protection and operating environment for these assets.

2 Introduction

Physical security measures must be in place to ensure physical integrity and access security of computer facilities. Protection measures must be appropriate to the classification level of the assets and information processed, stored, and handled within.

3 Secure areas

3.1 Delivery of equipment

3.1.1 The personnel responsible for the delivery of any IT equipment must supervise all accesses. This includes, but is not limited to:

- Supervising any delivery personnel;
- Controlling delivery personnel’s physical access to ‘secure areas’;
- Registering all visitors, delivery personnel and incoming equipment; and
- Securing physical access to the ‘secure areas’ after the delivery is completed.

3.2 Employee relocations

3.2.1 Moving of high sensitive information and personal equipment will be done or supervised by the employee rather than allowing them to be moved with the rest of the employee's possessions.

3.2.2 Individuals involved in workspace relocations will inspect their work area and furniture to ensure that no information has been left behind. Care will be taken to assign responsibility to all common file areas (e.g. hall file cabinets, file rooms, closets, storage rooms, etc.).

3.3 Physical entry controls

3.3.1 Employees and visitors must be authorised for physical entry into ‘secure areas’.

3.3.2 Doors to ‘secure areas’ must be locked at all times with only authorised personnel having the ability to enter via a secure access control system using smart cards or other similar means which is capable of capturing audit trails and imposing access time restrictions. Less secure means using only conventional keys or combination locks should be avoided.

3.4 Physical security perimeter

3.4.1 Physical security measures must be implemented to provide protection of ‘secure areas’ that contain sensitive computing facilities.

Security measures should be appropriate to the risk classification of facilities and systems located within.

'Secure areas' would include, but not limited to:
- Computer data centres;
- Network and communications room; and
- Equipment or media storage facilities.

3.4.2 For all 'secure areas', a security perimeter must be established. The strength of the security perimeter will be determined by an assessment of the risks and threats to the physical environment. Establishing the security perimeter includes, but is not limited to:
- Ensuring that the location of the facility has been appropriately selected to avoid threats such as flooding, motor vehicle accidents etc.;
- Ensuring all physical perimeter components (walls, doors, windows, etc.) are physically sound;
- Ensuring that all physical access to the computing facility is controlled;
- Implementing alarmed fire control doors; and
- Complying with all applicable safety regulations.

3.5 Securing offices, rooms and facilities

3.5.1 An up-to-date list of personnel who possess the cards/keys shall be maintained. The list should indicate the access privileges granted and time restrictions enforced, where appropriate.

3.5.2 Access to 'secure areas' must be reviewed every twelve (12) months to ensure that access privileges have been appropriately restricted to authorised personnel and time restrictions have been enforced where appropriate.

3.5.3 Dual control over the inventory and issue of access cards/keys to 'secure areas' shall be in place.

3.5.4 Loss of access cards/keys must be immediately reported to the issuing body so that appropriate action can be taken quickly to prevent unauthorised access.

3.5.5 All visitors shall sign in and sign out in a register and be escorted by authorized personnel at all times when accessing server room and wire centre. All visitors must not be allowed access into those areas without the approval by respective manager.

3.5.6 Emergency exits shall be tested periodically to ensure that the access security systems are in proper operating conditions.

3.5.7 Access to any areas within the data centre should be monitored 24 hours a day. This monitoring can be by cameras, alarmed doors and windows, personnel manning the centres, or a combination of the above. This monitoring serves as a deterrent against intrusion attempts and insures that unauthorised physical access to critical resources and information can be detected timely.

3.5.8 Any hazardous or combustible materials must be stored at a safe distance from any ‘secure area’ in accordance to safety regulations and manufacturer specifications.

3.5.9 All doors and windows accessible by public and leading to ‘secure areas’ must be locked when unattended and comply with any local safety regulations.

3.5.10 Rooms containing wiring or communications equipment (wiring closets, PBX rooms, etc.) must be locked at all times using card access systems or conventional key locks with access restricted to authorised personnel only. Signs should not be posted on wiring closets, telephone rooms and other equipment components that would attract the attention of unauthorised individuals.

3.5.11 The data centre must be equipped with doors that automatically close after they have been opened (door-closer). An audible alarm should be triggered when the doors have been kept open beyond a certain period of time.

3.5.12 To avoid unnecessary human traffic and physical damage to equipment, the data centre and network rooms should not be used for printing, faxing, and storage of computers, computer parts or stationary.

3.5.13 ‘Secure areas’ should not be shared with unauthorized personnel.

3.5.14 Backup and recovery media and facilities must be located at a safe distance from main facilities. The backup facilities must be at a distance that would protect it from damage from any incident at the main site.

3.6 Working in secure areas

3.6.1 Any person working or having access to a 'secure area' must be informed of the enhanced security requirements of the 'secure area', the details of the security perimeter of that area and the associated responsibilities for the area.

3.6.2 Photo taking and video recording is not allowed unless specifically authorised by the relevant head of department.

3.6.3 Any third party access granted to a 'secure area' must be strictly controlled and monitored. All parties with access to the area must be authorised and logged. This includes support services such as cleaning or waste removal.

4 Equipment security

4.1 Cabling security

4.1.1 Ethernet ports or network cabling must not be left unprotected in areas open to public access. All network connections must be removed and/or deactivated when premises are vacated.

4.1.2 Power and telecommunications equipment and cabling must be protected against deliberate or accidental interruption of service. This includes protecting control boxes, cables, wireless access points, cable risers, wiring hubs and other equipment from fire, vandalism, and interception of communications or disruption of service.

4.2 Equipment Maintenance

4.2.1 Equipment must be correctly maintained to ensure availability and to protect the integrity and confidentiality of information. In accordance with manufacturer's specifications, equipment should be monitored and inspected. Only authorised maintenance personnel should be allowed to perform repairs and all repairs or service work must be recorded. If equipment must be sent offsite for repairs, the confidentiality and integrity of any information must be ensured.

4.3 Power supplies

4.3.1 Uninterruptible Power Supplies (UPS) must be used for equipment supporting critical business operations to orderly shutdown or allow systems to continue running. UPS equipment should be checked half-yearly to ensure it has adequate capacity and tested in accordance with the manufacturer's recommendations.

4.3.2 Operational site personnel should be trained to monitor and control the various power supply equipment and devices.

4.3.3 Periodic inspection, testing and maintenance of the power equipment and systems should be scheduled.

4.3.4 To avoid power failures, a suitable electrical power supply must be provided in such a way that single point of failure can be avoided. Based on business criticality, the use of a back-up generator should be considered.

4.4 Removal of equipment

4.4.1 Employees or contractors must not remove equipment off the University’s premises, without prior authorisation from the department. All individuals must be aware that spot checks can take place without any advanced notice given. Any equipment that is removed must be logged out and logged back in a proper register for tracking of movements.

4.5 Equipments/medias in transit

4.5.1 Equipments in transit include mobile devices, medias, etc, where the equipments are not in their designated secure office environment. Users are to exercise due diligence to secure equipments in transit to prevent them from being misplaced or stolen.

4.6 Secure disposal or re-use of equipment

4.6.1 Any information processing equipment that is to be disposed of, or reused, must undergo a cleansing process before release. The cleansing process must consist of destruction of the information residing on equipment and testing of the process to ensure no data is left on the equipment.

4.7 Security of equipment off-premise

4.7.1 Off-premises equipment used to process NUS information must comply with NUS IT Security Policy, security standards and guidelines.

Authorised equipment and media taken off premise or outside NUS premises must be controlled, secured, and protected.

4.8 Site of equipment and its protection

4.8.1 All equipment must be sited in a manner or location to minimise risks or threat. This includes, but is not limited to:

- Threats of theft or vandalism;
- Risk of fire, explosion, smoke, flooding, chemical agents;
- Loss of services such as power, communication or water; and
- Any other physical or environmental threats

4.8.2 'Secure areas' must be constructed so they are protected against fire, water damage, vandalism, and other threats known to occur, or that are likely to occur at the involved locations.

4.8.3 Smoking, drinking and eating in computing facilities should be prohibited.

4.8.4 Automatic fire detection and fire suppression systems with audible alarms should be installed.

4.8.5 Fire extinguishers should be installed and their locations clearly marked with appropriate signs.

4.8.6 Fire suppression systems should be non-water based to minimise risk of equipment damage.

4.8.7 Fire-rated walls surrounding computing facilities must be non-combustible and resistant to fire for at least one hour. All openings to these walls (doors, ventilation ducts, etc.) should be self-closing and likewise rated at least one hour.

4.8.8 To minimise theft and water damage, computing and communications facilities should ideally be located above the first floor in buildings.

4.8.9 Computer equipment should operate in a climate-controlled atmosphere at all times. Backup ventilation plans must be provided in the event that air conditioning systems fail.

4.8.10 Procedures must exist for facilities management to monitor and test fire suppression system/equipment at least every six (6) months and document the test results.

4.8.11 Designated computing facilities personnel must be trained in the use of any automatic fire suppression systems, the use of portable fire extinguishers, and the proper response to smoke and fire alarms.

4.8.12 Procedures for the safe evacuation of personnel in an emergency should be visibly posted throughout the operational site. Periodic training and fire drills should be conducted.

5 General controls

5.1 Clear desk standard

5.1.1 All confidential information must be properly archived into secure file cabinets, closets or storage rooms after use. If the confidential information is not to be either used or archived, it must be shredded.

5.1.2 All printed documents (printers, faxes and photocopies) must be collected by employees. Printers, fax machines and photocopiers must be checked regularly (at least every day after business hours) for prints, which are not collected. The items should be kept secure until the proper owners of the documents are available.

5.1.3 All information on whiteboards or work boards must be erased after use.

5.1.4 All information storage media (such as hard disk drives, floppy disks, magnetic tapes, and CD-ROMs) containing executive, operational, and development data must be physically secured when not in use.

5.2 Clear screen standard

5.2.1 A PC or terminal must not stay logged on while unattended. In this case, access to the PC or terminal must be temporarily blocked, e.g. through the keyboard protection facility or screensaver password.

5.2.2 Where necessary and possible, measures must be taken to ensure that after a specific period of time during which the user has not used the PC or terminal:

- The PC or terminal will be logged off automatically; or
- The screen will turn dark or a screensaver activated, to preclude the possibility of further use without the password being re-entered.

Chapter 7 NUS IT Security Policy: Network Management

1 Purpose and scope

The purpose of this chapter is to establish standards that aim to reduce the risk of introducing security loopholes during design, implementation and maintenance of the network infrastructure. It also states the safeguards that should be in place for communication and exchange of information, either within NUS facilities and systems or external to NUS, to prevent unnecessary disclosure or loss.

2 Introduction

Effective network management is essential for maintaining a high level of service availability to users. Proper standards and procedures are also critical for ensuring the confidentiality and integrity of information transmitted across the network to prevent unauthorised disclosure or tampering of information.

3 Network management

3.1 Firewalls

3.1.1 Firewalls should be installed at the perimeter of the University's network that connects to the Internet and also between NUS internal networks and the Demilitarised Zone (DMZ).

3.1.2 If there is a need to separate the internal network into varying level of security, firewalls should be utilised to enforce such segmentation.

3.1.3 Firewalls should be configured according to the relevant technical controls.

3.2 Intrusion detection system (IDS)

3.2.1 Intrusion Detection Systems (IDS) should be deployed to provide real-time alert of possible attacks and intrusion.

3.2.2 The selection and placement of IDS should be based on the requirements and current infrastructure of NUS.

3.2.3 Network-based IDS should be used to monitor the inbound traffic to server farm segments.

3.2.4 The latest attack signatures of the IDS must be installed as soon as they are released.

3.2.5 IDS should be configured to provide real-time alerts when abnormal activities are detected, else IDS logs should be checked for critical incidents.

3.3 Network management procedures

3.3.1 Network infrastructure managers must ensure proper operational network controls are implemented. This includes:

- Documented roles and responsibilities for network operations;

- Procedures for management of equipment, both local and remote;
- Proper availability for network operations and services;
- Consistent controls applied across the University;
- Proper data integrity controls when data is passed over public network or communication lines; and
- Proper data confidentiality controls.

3.3.2 All non-emergency changes to NUS network infrastructure must follow NUS change management standards. Changes to internal networks include loading new software, changing network addresses, reconfiguring routers, adding dial-up lines, creating trusted host relationships, and the like.

3.3.3 For emergency changes, the network or system administrator will have to seek approval from the relevant project or Network Manager.

These changes must be clearly and completely documented and approved within 24 hours of resolution of the problem. This process shall prevent unexpected changes from inadvertently leading to denial of service, unauthorised disclosure of information, and other problems.

3.4 Routers

3.4.1 All routers should be configured according to the relevant technical controls guidelines.

3.4.2 Router packet level filtering using access control lists should be enabled and configured in the absence of firewall perimeter protection or to reinforce firewall protection. These access control lists should be setup to prohibit restricted services, protocols, etc.

4 Exchanges of information and security

4.1 Information disclosure

4.1.1 Every user must be conscious of disclosing confidential information in conversations, Instant Messaging or other forms of communication. Examples of good practices are:

- Do not discuss confidential information in public places;
- Never open pictures, download files, or click links in instant messages from strangers;
- Do not reveal confidential materials while working on laptops in public places; and
- Do not leave confidential information in voicemails.

4.2 Security of electronic mail (e-mail)

4.2.1 Policies on the acceptable usage of e-mail should be documented. New staff must accept the Acceptable Use Policy, containing e-mail related policies, upon issuance of NUS e-mail account to signify their consent to the policy.

4.2.2 E-mail messages must be considered to be the same as formal, written NUS memoranda. Hence e-mail messages are considered part of NUS records.

4.2.3 Every user shall comply with AUP on the appropriate use of NUS Email.

4.2.4 NUS standard footers for email should be configured on the email server to be appended to all official emails sent outside of NUS wherever appropriate.

4.3 Security of electronic office systems

4.3.1 Printers and copiers must not be left unattended when sensitive data is being printed or copied. Persons monitoring these processes and/or having access to these devices must be authorised to examine the data being printed. All waste that is generated in the course of printing or copying such data must be destroyed in accordance with proper disposal standards.

4.3.2 Fax machines must not be left unattended when sensitive data is being faxed. Persons monitoring these processes and/or having access to these devices must be authorised to examine the data being printed. All waste that is generated in the course of faxing such data must be destroyed in accordance with proper disposal standards.

4.3.3 Information sent via fax must include NUS fax cover page with a disclaimer that the information sent is for the use of the intended recipient only.

4.4 Security of media in transit

4.4.1 When transferring media, such as CDs, tapes or diskettes, containing sensitive information, the media must be placed in sealed envelopes with the name of the intended recipient clearly marked.

4.4.2 Any media, such as CDs, tapes or diskettes, sent by postal service or courier must be protected from unauthorised access, misuse or corruption. Employees must ensure packaging for information is sufficient to protect contents from physical damage or tampering. For sensitive information, special controls must be used including, but are not limited to:

- Tamper resistant packaging;
- Delivery by hand; and
- Delivery upon signature verification.

4.5 Security of system interfaces:

4.5.1 Transfer of data between systems shall be initiated after successful authentication.

4.5.2 Confidential data transfer between system should be secured (e.g. session management) and encrypted or sent over encrypted channel (e.g. sftp, ftps, https).

4.5.3 Confidential data should be erased from staging system (e.g. ftp folders, web server folders) when data has been transferred to destination. system.

4.5.4 Data file should be scanned for virus before uploading or downloading to system.

4.6 Vulnerability scanning and disconnection policy

4.6.1 The IT Security should conduct periodic network vulnerability scanning of servers within NUS. If vulnerabilities are identified, the IT Security group should notify the appropriate System administrators immediately. System administrators should respond to vulnerability scanning alerts as soon as possible.

4.6.2 Depending on the severity of the situation, the IT Security group may initiate disconnection of compromised/vulnerable machines.

Chapter 8 NUS IT Security Policy: Operations Management

1 Purpose and scope

The purpose of this chapter is to establish standards that aim to reduce the risk of errors and security compromises occurring during systems processing by careful control of system operations.

2 Introduction

Proper operations management of information resources and systems is necessary to ensure that day-to-day operations and usage of NUS systems is efficient and to minimise the risk of security compromises.

3 Operational procedures and responsibilities

3.1 Documented operating procedures

3.1.1 Procedures for job execution should be documented and include the following:

- System restart and shutdown procedures;
- Jobs scheduling and dependencies. This documentation must include job start times, latest job completion times, delay procedures and handling procedures in case of failure or error;
- Third party support contact list;
- Handling of errors and exceptions;
- Secure disposal of hard copy printouts; and
- Any special instructions.

3.1.2 Housekeeping procedures should be documented and include the following:

- Start-up and shut down procedures;
- Back-up and recovery; and
- Equipment and facilities maintenance.

3.1.3 Changes to the procedure documents have to be authorised by the respective Managers overseeing the operations.

3.2 Operation change control

3.2.1 Changes in information processing facilities and systems should be performed in accordance to change controls procedures.

3.3 Segregation of duties

3.3.1 Where feasible the following IT duties should be performed by separate groups/employees:

- IT management;
- Software development;
- Program promotion/migration;
- Systems operations/daily administration;
- Application and end-user administration;
- Helpdesk/support; and
- Network management.

In addition, controls must be deployed to mitigate any activities that would circumvent any procedural restrictions or business process operations. Any activity that could result in fraud or misuse to NUS information or systems must have mitigating controls for separation of duties or the implementation of controls to detect fraud or misuse.

3.4 Separation of development and operational facilities

3.4.1 Separate environments must exist for the following:

- Development;
- Testing;
- Production

3.4.2 The production environment is where the production executable code for an application will reside. Only a non-developer designated as the release engineer, who is authorised by the Application Owner, will have write access to these libraries. Application developers will have read-only access.

3.4.3 Compilers and other system development tools should not be installed on the production environment. If however these are necessary, then access and execution rights for compilers and other system development tools installed on the production environment must be strictly controlled.

3.4.4 Login screens for production and development should be different. The login screen for a production system or application should include a notification that it is a production environment.

4 System planning and acceptance

4.1 Capacity planning

4.1.1 All information systems should be able to cater to anticipated capacity requirements. It is the responsibility of the system's development and operational teams to determine anticipated capacity and hardware requirements. This includes, but is not limited to:

- Disk usage and size;
- Network traffic load;
- Load balancing requirements;
- Processing power; and
- Memory requirements.

4.1.2 Network and System Administrators should monitor network and system utilization reports to facilitate capacity planning to ensure IT systems availability is not disrupted by system capacity issues.

4.1.3 Major systems capacity planning exercise should be carried out for all IT systems every twelve (12) months for budget planning and resources allocation.

4.1.4 Redundancy should be available for equipment and systems supporting critical business operations to ensure availability of data.

4.1.5 Servers which provide key services should be dedicated, and should not provide auxiliary services.

4.2 System acceptance

4.2.1 It is the responsibility of the Project Manager to ensure that new or updated systems shall only be accepted when all the requirements defined in Chapter 10, Clause 3.1.1 are fulfilled.

5 Protection against malicious software and viruses

5.1 General responsibilities

5.1.1 Users must not execute any unknown files, especially if it is not from a trusted and reliable source. Even though it may not contain a known virus, executable files downloaded from the Internet or other unsecured locations can cause damage or introduce vulnerabilities.

5.1.2 User possession or development of viruses or other malicious software is strictly prohibited.

5.1.3 In the event of a virus infection or outbreak, the IT Security group, with the assistance of Network and System Administrators, must determine the origin of the virus infection and whether any other computers have been infected. This insures that the total problem is addressed and computers are not constantly being re-infected.

5.2 General standards

5.2.1 E-mail attachments and files downloaded from the Internet should be scanned at the mail or Internet gateways, and suspicious content should be quarantined.

5.2.2 All PCs and notebook/laptop users must be equipped with up-to-date virus screening software.

5.2.3 PCs must be scanned regularly, and the anti-virus software must remain resident throughout the computing session. The complete hard drive should be scanned at every month.

5.2.4 Virus scanners and/or detection programs must be installed on all Information systems. These programs should be configured to provide real-time protection and should be updated regularly to scan for new strains of viruses.

6 Logging and backup

6.1 Fault logging

6.1.1 Operational personnel must log all reports of errors or problems with information processing or communication systems. The log must include:

- Name of person reporting fault;
- Date/time of fault;
- Description of error/problem;
- Name of party responsible for problem resolution;
- Description of initial operations response;
- Name of operations person entering fault report;
- Description of problem resolution; and
- Date/time of resolution.

6.1.2 Fault logs should be reviewed daily for consistency and proper documentation. Open errors or issues must remain open until satisfactorily resolved. Also, these logs must be archived and available for independent verification.

6.2 Information back-up

6.2.1 System Administrators must develop off-site backup rotation and retention and data archival schedules for each application that they support, based on requirements set forth by the System Owners. The schedules must reflect the risk assessment of the information being stored. System administrators are also responsible for ensuring that backups of software on the servers are performed and that off-site storage standards are followed.

6.2.2 The operations personnel must ensure that all information is backed up and available to be restored in the case of an emergency.

6.2.3 Each system must have documented backup and recovery procedures.

6.2.4 The administrators must ensure that annual restorations of tape backups are performed. The purpose of the annual restoration is to test the capability of restoring tape backups and also to ensure that the backup tapes are still serviceable. Only administrators or operators are authorised to recall backups and restores based on requests from authorised System Owners. Restoration testing must be performed with live production backup data on the test systems in the test environment only. Test data must be properly protected according to Chapter 10, clause 6.3.1.

6.2.5 Information systems data or functions are considered non-critical data if the unavailability of that information poses no disruption or minimal disruption of service to customers and vendors. Such information will be backed-up periodically and periodically moved to a secure off-site location.

6.2.6 Information systems data or functions are considered critical data if the unavailability of the information would completely interrupt the business from functioning (i.e., the process cannot be performed manually) and impact would be highly adverse. Such information must be backed-up daily and stored in a suitable off-site location. Consideration must be made as to whether incremental backups must occur between daily backups.

6.2.7 Users of personal computers are responsible for performing backups of their own critical files.

6.3 Operator logs

6.3.1 Operations staff responsible for any information processing must keep a log on all operational and production activities. This log must include, but is not limited to:

- Date/time of activity;
- Activity description;
- Error handling and action/resolution, if applicable;
- Verification of proper operational procedure; and
- Name of operations staff.

6.3.2 Operations logs should be reviewed periodically for consistency and proper documentation. Also, these logs must be archived and available for independent verification.

7 Media handling and security

7.1 Disposal of information and media

7.1.1 Electronic information storage media must be disposed of in a manner commensurate with the information classification stored there.

7.1.2 Storage media that contain sensitive data must be 'securely wiped'.

7.2 Information handling procedures

7.2.1 Physical access to system data must be restricted to staff whose job responsibilities require access. This authorisation list for access to media must be reviewed periodically by the Data Manager for appropriateness.

7.2.2 Any data or media waiting to be distributed or produced must be secured to a level consistent with its sensitivity. This includes, but is not limited to:

- Printer spools on systems;

- Printed materials awaiting distribution;
- Printed materials awaiting pickup for external delivery services; and
- Media, such as backup tapes, awaiting pickup for offsite storage.

7.2.3 Recipients of data must be clearly marked. Any media sent via inter-office mail, courier, or other means, must be clearly labeled with the appropriate recipient information.

7.3 Management of removable computer media

7.3.1 Critical media containing aggregated NUS Confidential or NUS Restricted information must be stored in a secure manner. This includes physical security to prevent theft, and environmental controls to prevent media degradation.

7.3.2 Any computer media leaving NUS facilities must be authorised by the appropriate management. Media containing aggregated NUS Confidential or NUS Restricted information should be accounted for with a movement log.

7.4 Security of system documentation

7.4.1 System documentation must be controlled and protected against unauthorised access. Access to the documentation must be kept to a minimum and only individuals needing the documentation per their job responsibilities will be given authorisation. Such documentation includes, but is not limited to:

- Operational procedures;
- System and application documentation; and
- Operations and production logs.

Chapter 9 NUS IT Security Policy: Incident Management

1 Purpose and scope

The purpose of this policy is to define a structured approach in managing security incidents to reduce the potential damage caused by security breaches.

2 Introduction

Incident management is essential to ensure appropriate actions are taken when security breaches occurs. It depicts the necessary precautionary controls to be put in place to ensure a structured approach to managing security incidents. The detailed process of handling security incidents shall be documented in the NUS Incident Response Plan.

3 Operational procedures and responsibilities

3.1 Security incident management procedures

3.1.1 IT security incident is a violation of organisation's security policies or standards. These activities include but are not limited to:

- Successful or failed attempts to gain unauthorised access to a system or its data;
- Unauthorised use of a system or network for the processing or storage of data;
- Changes to the integrity of a system or network without knowledge, instruction or consent from the owner;
- Unwanted disruption or denial of service of a system or network; and
- Unauthorised collection of information for facilitating future intrusion attempts or espionage purposes.

3.1.2 Users and contractors shall report all security incidents immediately upon discovery, following the process laid out in the NUS Information Security portal.

3.1.3 For incidents or threat, evidence must be collected and integrity of evidence is maintained so that appropriate legal action can be taken, if deemed necessary.

3.1.4 The IT Security Group must maintain a database or records containing security incidents handled.

3.2 Security incident response team

3.2.1 The IT Security Group is responsible for following up on the reported issues in a swift and confidential manner.

3.2.2 IT Security Group must work with the affected department's System Administrators, Network Administrators, Data Managers and System Owners, as according to NUS incident response plans.

3.2.3 The System Administrator, System Owner and/or Data Manager will be identified to assist the Incident Response Team in the discharge of its duty. If a threat, or potential threat, has been identified to specific systems, data or processes, the System Administrator, System Owner and/or Data Manager shall be consulted to assist in 'quantifying' the impact to NUS operations. This will aid in the management of the incident and also provide insight on damage or recovery costs.

4 Responding to security incidents

4.1 General responsibilities

4.1.1 If a user suspects a security weakness or notices an area of exposure to NUS security, the employee must notify the IT Security Group.

4.1.2 If a security incident is suspected or noticed by any employee, the user must immediately notify the IT Security Group.

4.1.3 Once the IT Security Group has discovered, or been notified of, a security incident involving a server, the system administrators shall be notified.

4.2 General standards

4.2.1 A process to periodically review the Incident Response Plan, document "lessons learnt" and co-ordinate training and learning sessions should be implemented.

Chapter 10 NUS IT Security Policy: System Development and Maintenance

1 Purpose and scope

This chapter covers standards relating to systems development and maintenance of NUS infrastructure, business applications and end-user applications.

2 Introduction

Proper design, implementation and maintenance of Information Systems are crucial towards security. Security requirements should be identified at the requirements phase of a project and agreed prior to the development of information systems.

These requirements must address every phase of the system development life cycle including design, development, maintenance and operations phases.

3 Security requirements of systems

3.1 Security requirements analysis and specification

3.1.1 For all systems developed within or for NUS, security requirements must be determined prior to actual development of the system. During the requirements gathering and design phase, System Owners and Project Manager must determine the desired controls based on a risk assessment study. These security requirements should include but are not limited to:

- Authentication;
- Access control;
- Accounting and audit logs;
- Non-repudiation;
- System availability;
- Data confidentiality and integrity;
- Compliance with applicable legal or regulatory requirements
- Performance and computer capacity requirements;
- Contingency planning;
- Training requirements for operational and user support;
- Adherence to NUS application development and maintenance methodology; and
- Conduct of pre-implementation system hardening and security review.

4 Security in application systems

4.1 Control of internal processing

4.1.1 To detect corruption of data due to processing errors or malicious acts, validation checks including the following should be built into key applications:

- Session or batch controls that automatically alerts and prevents the batch job from continuing if a previous program in the batch run encounters errors;
- Output checking, for example to validate that the calculated value is within a tolerance limit;

- Sequence checking, for example to ensure the output is in the desired order; and
- Maintenance of hash totals to ensure completeness of processing.

4.2 Input data validation

4.2.1 Data input to applications should include data validation checks including:

- Error detection, such as hash totals and missing values;
- Checks for invalid characters or inconsistent data (e.g. text in number fields); and
- Logical inaccuracy, e.g. impossible dates or contradiction; and
- Any other business requirements.

4.3 Output data validation

4.3.1 Where information is output from a computer system, system checks must be performed to ensure it is:

- Complete - via reconciliation controls;
- Accurate – via plausibility checking or sample checking; and
- Only available to appropriate recipients.

4.4 Secure Coding

4.4.1 Secure coding guidelines shall be adopted in each phase of the software development life cycle.

4.5 Website Vulnerability Scan

4.5.1 The IT Security group should conduct periodic vulnerability scanning of websites within NUS. If vulnerabilities are identified, the IT Security group should notify the appropriate IT Support Personnel promptly. The IT Support Personnel should respond to vulnerability scanning alerts as soon as possible.

5 Cryptographic controls

5.1 Key management

5.1.1 Cryptographic keys must be managed and protected effectively, in accordance to industry standards (such as PKCS and FIPS 140-1). This protection must include:

- Creation and issuance of keys;
- Confidentiality of private keys;
- Integrity of public keys;
- Revocation of keys;
- Recovery of lost keys;
- Archiving of old keys; and
- Destruction of keys which are no longer needed.

5.1.2 Master key generation needs to be very secure as all other keys are derived by the master key. At a minimum, dual access control mechanisms should be implemented to provide protection for the master key.

5.2 Use of cryptography

5.2.1 Cryptography shall be applied in the following conditions:

- Based on Data Classification Guidelines; and
- Financial/Transactional information exchanged over public networks.

5.2.2 Where cryptographic controls are required, they shall be applied on both storage and transmission whenever applicable.

6 Security of system files

6.1 Access control to program source library

6.1.1 Libraries/directories containing production source codes must be secured from unauthorised access using the following controls:

- Source codes should not be held on production systems where possible;
- Librarians for each application should maintain an audit log of accesses;
- File system access rights and change control procedures should be implemented to prevent IT staff from gaining access to source codes in an uncontrolled manner;
- Production source libraries should be separated from development source libraries; and
- Authorisation procedures should be implemented for updating program source libraries.

6.2 Control of operational software and codes

6.2.1 All production application and system software must be secured from unauthorised amendments or deletion. Wherever possible the source and compiled application codes must be stored in system libraries/directories with update permissions restricted to the appropriate operations team only. The code must be version controlled and replaced only after receipt of approved program promotion documentation. An audit log of all updates to the software and a library of previous versions must be maintained.

6.2.2 All changes to operational software must be performed while observing the program change controls.

6.2.3 There must only be one repository for production source code. Developers must retrieve the source code from this repository when modifying programs. All modifications to production source code must follow strict version control guidelines.

6.3 Protection of system test data

6.3.1 Where operational data is copied to a test system it must be subject to a similar level of control as the live version. The controls must include:

- Authorisation for the use of the production data set;
- Erasure after testing has been completed;
- Sanitization of sensitive data;

- Capture of activity and access audit logs on the test system; and
- Access controls to ensure confidentiality is maintained.

7 Security in development and support processes

7.1 Change control procedures

7.1.1 The roles and responsibilities for individuals involved in the change control process must be clearly defined and incompatible responsibilities should be properly segregated.

7.1.2 A group or individual independent of programming should be responsible for the migration of the changed program from test library to production library.

7.1.3 Change requests must be properly documented using approved Change Request Forms.

7.1.4 Change requests have to be approved by the System Owners / project managers of all affected applications before implementation can commence. System Owners are responsible for ensuring that security risks arising from the change requests have been properly assessed and addressed. Delegation of the above role is permissible. However the responsibilities still lie with the System Owner.

7.1.5 Completed change request forms, test plans and results should be retained for a period of at least three (3) years for tracking purposes.

7.1.6 Test plan and results must be properly documented. If problems are noted during the testing process, the developer will document the problem, make appropriate modifications in the development environment and submit it to the operations team, with approval from the relevant supervisor, for retesting.

7.1.7 All change requests shall be tested with the test results reviewed and accepted by all concerned parties, including users and System Owners, prior to implementation.

7.1.8 Tests should be performed in a controlled environment. Prior to the test, the following should be agreed by concerned users and System Owners:

- Test objectives;
- Test acceptance criteria; and
- Test plan activities.

7.1.9 Sensitive production data shall not be used for testing.

7.1.10 Test data used should be comprehensive and should be extended, if necessary, to test new or changed processing functions.

7.1.11 Tests should be done for the complete system to ensure the correct interaction between the updated programs and other programs.

7.1.12 System and application software backup must be performed before system upgrades and/or maintenance occurs.

7.1.13 An independent review of program changes should be conducted before the programs are moved into a production environment to detect unauthorised or malicious codes.

7.1.14 Fall-back procedures in the event of a failure in the implementation of the change process shall be established prior to implementation.

7.1.15 Existing system documentation must be updated (program, operations and user documentation) to accurately reflect program changes. Where necessary, a briefing or training session shall be given to staff affected by the changes.

7.1.16 Source code of different versions should be stored off-line using version control software which can capture the relevant details and compare source code and identify changes.

7.1.17 Access levels must restrict developers from making changes to the code maintained in the test environment during acceptance testing.

7.1.18 The access privileges of developers to production libraries must be restricted, such that they will only be permitted to copy source code.

7.2 Covert channels and trojan code

7.2.1 Controls to prevent application codes from having covert channels or Trojan Code should be implemented. These controls should, to the extent possible, include:

- Buying programs only from a reputable source;
- Using evaluated products;
- Controlling access to, and modification of, code once installed;

7.3 Emergency change controls

7.3.1 All emergency requests will be documented in an incident or trouble log.

7.3.2 Under normal circumstances, the designated release engineer must install emergency fixes. In rare cases where programmers require update access, special temporary accounts or access may be created with the approval from the System Owner. These temporary accounts must be disabled or deleted upon completion of the emergency session.

7.3.3 Using the security features available by the systems, automated audit trail of all emergency activities must be generated. At a minimum, the logs should identify the person making the change, time and date, the commands executed, the program and data files affected.

7.3.4 Production source code should not be changed in response to an emergency change request. Instead, a controlled temporary version or a patch must be created and executed until the production source can be changed and the executable updated.

7.3.5 Only those persons authorised by the System Owner can make emergency changes to the information resources directly. These changes must be clearly and completely documented and approved within 24 hours of resolution of the problem at which time a permanent course of action will be determined.

7.3.6 A decision as to whether to back-out the emergency fix or allow it to remain in effect until a permanent fix is available will be made jointly by the project manager and the System Owner. Where a permanent fix is needed, it must be subjected to the normal change request process.

7.3.7 The person making an emergency change on security areas must provide a written description of what was done to address the emergency to project manager and /or System Owner.

7.4 Restriction of changes to software packages

7.4.1 Changes to software packages should be minimized to reduce the risk that built-in controls may be compromised. Where significant customisation has to be done, an assessment of the impact of the changes on the built-in controls should be performed, assisted by expertise from the product vendor or otherwise. Such customisation should be documented.

7.4.2 All significant modifications, major enhancements to software packages must be tested in a controlled development environment prior to installation of the software in production. System stress testing and volume testing must be performed, and in some cases, parallel testing, if required, should be performed.

7.5 System patches

7.5.1 A procedure to monitor system patches released by product vendors should be in place. Relevant patches have to be tested and subsequently applied to production systems on a timely basis.

7.6 Technical review of operating system changes

7.6.1 A review and application tests should be performed when operating system version updates, patch updates or significant configuration changes are made. Tests should be comprehensive to ensure that the changes do not impact the operations or security of the application. The process should cover, but are not limited to:

- Ensuring that notification of operating system changes is provided in time to allow appropriate reviews to be conducted by relevant parties before implementation;

- Reviewing of the changes to ensure that they do not compromise application controls that rely on the operating system settings; and
- Ensuring that users are involved in the testing and all critical system functionality are tested.

Chapter 11 NUS IT Security Policy: Compliance

1 Purpose and scope

This chapter defines the actions necessary for ensuring compliance with legal and regulatory requirements, NUS IT Security Policy as well as all other NUS approved security standards and guidelines.

Legal and regulatory requirements may include any criminal or civil law, statutory, regulatory or contractual obligations made on behalf of the University.

2 Introduction

The University's Information Systems are subjected to various legal and regulatory requirements as well as procedural and technical security standards defined in this IT Security Policy and any other NUS approved security standards and guidelines.

Ensuring compliance to all these requirements is necessary for an effective security program.

3 Compliance with regulatory requirements

3.1 Identification of applicable legislation

3.1.1 All applicable legal, statutory, contractual or regulatory requirements should be defined and documented for each information system.

Such requirements include, but are not limited to:

- Copyright Act;
- Patent Act;
- Trademark Act;
- The Evidence (Computer Output) Regulations in Chapter 97 of The Evidence Act;
- The Personal Data Protection Act;
- The Electronic Transactions Act; and
- The Computer Misuse and Cybersecurity Act.

3.1.2 Data Stewards should ensure that specific controls and responsibilities for meeting these regulations are defined and responsibilities assigned to the appropriate parties within NUS.

3.2 Intellectual property rights

3.2.1 The use or copying of purchased software so that it can be used on a computer other than the computer for which it is licensed is strictly prohibited.

3.2.2 Users of software on NUS information systems must strictly abide by copyright laws and restrictions imposed by the software manufacturer.

3.2.3 Computer software developed by or for NUS is the property of NUS. This policy must be conveyed to all third parties who develop software or applications for NUS, by stating it as a requirement in the contract. This prevents any dispute about ownership of the software once the project is complete. Software developed by NUS staff on company time becomes the property of NUS.

3.3 Prevention of misuse of information processing facilities

3.3.1 NUS information processing facilities are for authorised use only. Any use of the facilities for unauthorised purposes, without management approval, will be regarded as improper use of the facilities and should be brought to the attention of the relevant authorities for appropriate disciplinary action.

3.3.2 Monitoring of the usage of information processing facilities must not infringe any laws and regulations.

4 System audit considerations

4.1 Protection of system audit tools

4.1.1 All audit tools, including software and data files required for system audits must be protected from possible misuse or compromise. These tools should be protected with restricted access controls to authorised users only.

4.2 System audit controls

4.2.1 Audit activities must be properly planned to minimise any disruption or interruption of business operations. Planning activities include, but is not limited to:

- Agreeing on all audit activities and objectives with management;
- Limiting scope of assessment to a controlled environment and ensuring that no improper access is given to perform the audit tasks;
- Identifying resources and skills needed for any technical tasks; and
- Logging all audit activities and providing documentation of tasks performed, audit procedures, findings and recommendations.

All information on this site is classified as NUS Restricted