Policy Directive

Ministry of Health, NSW
73 Miller Street North Sydney NSW 2060
Locked Mail Bag 961 North Sydney NSW 2059
Telephone (02) 9391 9000 Fax (02) 9391 9101
http://www.health.nsw.gov.au/policies/

Electronic Information Security Policy - NSW Health

Document Number	PD2013_033
Publication date	11-Oct-2013
Functional Sub group	Corporate Administration - Information and data Corporate Administration - Security Personnel/Workforce - Security
Summary	The use of information and information systems is an integral part of most NSW Government activities. Electronic information assets are critical in agencies operations and are key element in delivering trustworthy government services. The security threats to information assets are increasing. The government has a duty to safeguard its large information holdings and must provide credible assurance that it is doing so.
Replaces Doc. No.	Electronic Information Security Policy - NSW Health [PD2008_052]
Author Branch	
Branch contact	Kavesh Moodley 8644 2726
Applies to	Local Health Districts, Board Governed Statutory Health Corporations, Chief Executive Governed Statutory Health Corporations, Specialty Network Governed Statutory Health Corporations, Affiliated Health Organisations, Public Health System Support Division, Community Health Centres, Environmental Health Officers of Local Councils, Government Medical Officers, NSW Ambulance Service, Ministry of Health, Private Hospitals and Day Procedure Centres, Public Health Units, Public Hospitals
Audience	All staff
Distributed to	Public Health System, Environmental Health Officers of Local Councils, Government Medical Officers, NSW Ambulance Service, Ministry of Health, Private Hospitals and Day Procedure Centres
Review date	11-Oct-2018
Policy Manual	Health Records & Information, Patient Matters
File No.	H13/5949
Status	Active

Director-General

This Policy Directive may be varied, withdrawn or replaced at any time. Compliance with this directive is **mandatory** for NSW Health and is a condition of subsidy for public health organisations.

POLICY STATEMENT

NSW HEALTH – ELECTRONIC INFORMATION SECURITY POLICY

PURPOSE

NSW Health is committed to the provision of appropriate levels of security across all of its information systems. Health information systems containing personal information are acknowledged as having particular security requirements, and are explicitly addressed in this policy.

This policy is based on a number of key principles. These are:

- NSW Health's major objective is the provision of health care services underlined by the overall welfare of the people it treats.
- All personal health information will be securely managed and that privacy and confidentiality will be preserved. The community must be confident NSW Health observes this principle.
- All other critical and sensitive information will also be securely managed and privacy and confidentiality maintained.
- Personnel have a responsibility for the security and maintenance of critical and sensitive information including personal health information.
- All other information must be classified[2] for the purposes of determining the level of security required as per Australian Government Security Classification System as represented within NSW Government - Digital Information Security Policy M2012-15.
- Providing information security education and developing awareness for all people dealing with electronic information is an integral part of maintaining adequate protection over that information.
- The release of information will comply with relevant and current state and federal legislation.
- The implementation of information security controls to mitigate the risks to sensitive information without impacting the timely provision of those services.
- It is also the responsibility of all NSW Health personnel and their contractors to be aware of and comply with the requirements of the NSW Health Privacy Manual Version 2 (PD2005_593) and the NSW Health Privacy Management Plan (PD2005_554).

Please refer to Sections 2 & 3 of the Electronic Information Security Policy which provide further guidance on the policy.

MANDATORY REQUIREMENTS

The Government's digital information systems security objectives as stated in the new Ministerial Memorandum (M2012-15) are:

- **Confidentiality** – to uphold authorised restrictions on access to and disclosure of information including personal or proprietary information.
- **Integrity** – to protect information against unauthorised alteration or destruction and prevent successful challenges to its authenticity.
- **Availability** – to provide authorised users with timely and reliable access to information and services.
- **Compliance** – to comply with all applicable legislation, regulations, Cabinet Conventions, policies and contractual obligations requiring information to be available, safeguarded or lawfully used.

- **Assurance** – to provide assurance to Parliament and the people of NSW that information held by the Government is appropriately protected and handled.

To meet the above requirements and provide appropriate assurance, implementation guidance is included as Appendix A of the policy.

IMPLEMENTATION

This policy covers security requirements for NSW Health information including electronic personal health information.

This policy applies to all employees, contractors and other persons who, in the course of their work, have access to information (including electronic personal health information) in or on behalf of the NSW public health system.

Please refer to the Section 4 titled 'Scope' of the Electronic Information Security Policy for implementation and scope of policy requirements.

Where access is granted to information held by the public health system for research or other purposes, the person or organisation granted access must, under the conditions of access, also be required to comply with the terms of this policy.

Compliance with this policy and all relevant acts and regulations as they relate to information security is mandatory for management, personnel and all persons handling electronic information, whether directly or indirectly involved in client service delivery.

All personnel and organisations referred to above should be aware of their legislative confidentiality obligations and that the breach of those obligations may result in prosecution and the imposition of a penalty or disciplinary actions.

REVISION HISTORY

Version	Approved by	Amendment notes
PD2013_033	Deputy Director General, Governance Workforce and Corporate	Electronic Information Security Policy v3.0 PD2008_052 has been updated in line with Premiers Memorandum M2012-15
PD2008_052	Director General	Electronic Information Security Policy Version 2.
PD2005_314	Director General	New Policy.

ATTACHMENTS

1. Electronic Information Security Policy - NSW Health.

Policy Directive

Ministry of Health, NSW
73 Miller Street North Sydney NSW 2060
Locked Mail Bag 961 North Sydney NSW 2059
Telephone (02) 9391 9000 Fax (02) 9391 9101
http://www.health.nsw.gov.au/policies/

Electronic Information Security Policy - NSW Health

Document Number	PD2013_033
Version Number	3.0
Publication date	11-Oct-2013
Functional Sub group	Corporate Administration - Information and data
Summary	NSW Health has an obligation to protect sensitive information such as that relating to patients and is committed to the provision of appropriate levels of security across all the electronic information systems it is responsible for. To address this obligation, all NSW Health organisations must implement the requirements of Ministerial Memorandum M2012-15 (Digital Information Security Policy). Current NSW Health policy on privacy and the relevant legislation must be taken into account when the above requirements are addressed by NSW Health organisations.
Replaces Doc. No.	Electronic Information Security Policy - NSW Health [PD2008_052]
Author Branch	Office of the CIO, NSW Health
Branch contact	**HealthShare NSW, Information Services,** Security
Applies to	Local Health Districts, Chief Executive Governed Statutory Health Corporation, Board Governed Statutory Health Corporations, Affiliated Health Organisations, Affiliated Health Organisations - Declared, Public Health System Support Division, NSW Ambulance Service, Ministry of Health
Audience	All providers of health services.
Distributed to	Public Health System, NSW Ambulance Service, Ministry of Health
Next Review date	11-Oct-2018
Policy Manual	Health Records & Information
File No.	H13/5949
Status	Active

Director-General
This Policy Directive may be varied, withdrawn or replaced at any time. Compliance with this directive is **mandatory** for NSW Health and is a condition of subsidy for public health organisations.

Policy Directive

Ministry of Health, NSW
73 Miller Street North Sydney NSW 2060
Locked Mail Bag 961 North Sydney NSW 2059
Telephone (02) 9391 9000 Fax (02) 9391 9101
http://www.health.nsw.gov.au/policies/

Table of Contents

1. Introduction

This document is Version 3.0 of the "NSW Health Information Security Policy" (PD2005_314).

The first version of this policy was issued on 8 July 2003 as Circular 2003/47 and published as a Policy Directive (PD2005_314) on 27 January 2005. The policy was developed following extensive consultation with a wide range of stakeholders, including significant input from clinicians.

The Second version of this policy was issued on 15-Sep-2008 as Premiers Memorandum M2007-04 and published as a Policy Directive (PD2008_052)

Publication of New Versions has become necessary for the following reasons:

- The applicable national standards relating to information security have changed (the new standards are AS/NZS ISO/IEC 27001:2006 and AS/NZS ISO/IEC 27002:2006);
- Government policy has been updated accordingly and the actions required of agencies in achieving the Government's objectives have changed. The updated policy is stated in Ministerial Memorandum M2012-15;
- The relevant NSW Health policies concerning the privacy of personal information have been updated. The updated policies are the "NSW Health Privacy Manual (Version 2)" (PD2005_593) and the "NSW Health Privacy Management Plan" (PD2005_554);
- To incorporate the changes in structure and requirement relevant to NSW Government Digital Information Security Policy Version 1.0 Released in Nov 2012 as Premiers Memorandum M2012-15
- As per scheduled periodic review cycle.

2. Information Security Policy Statement

NSW Health[1] is committed to the provision of appropriate levels of security across all of its information systems. Health information systems containing personal information are acknowledged as having particular security requirements, and are explicitly addressed in this policy.

This policy is based on a number of key principles. These are:

- NSW Health's major objective is the provision of health care services underlined by the overall welfare of the people it treats.
- All personal health information will be securely managed and that privacy and confidentiality will be preserved. The community must be confident NSW Health observes this principle.
- All other critical and sensitive information will also be securely managed and privacy and confidentiality maintained.
- Personnel have a responsibility for the security and maintenance of critical and sensitive information including personal health information.
- All other information must be classified[2] for the purposes of determining the level of security required as per Australian Government Security Classification System as represented within NSW Government – Digital Information Security Policy M2012-15.
- Providing information security education and developing awareness for all people dealing with electronic information is an integral part of maintaining adequate protection over that information.
- The release of information will comply with relevant and current state and federal legislation.
- The implementation of information security controls to mitigate the risks to sensitive information without impacting the timely provision of those services.

[1] In the context of this document the term NSW Health includes all NSW Health organisations. The NSW Health organisations are: Local Health Districts (Including public health units, public hospitals and Community Health Centres)/Chief Executive Governed Statutory Health Corporations, Board Governed Statutory Health Corporations, Affiliated Health Organisations – Health Administration Corporation (including HealthShare), Dental Schools and Clinics, NSW Ambulance Service, and the NSW Ministry of Health.

[2] All unclassified information should be treated as "For Official Use Only" information.

3. Privacy Statement

All public sector agencies in NSW, including the public health sector, are required to comply with the Privacy and Personal Information Protection Act 1998 and the Health Records Information Privacy Act 2002, which set out a series of rules designed to protect the privacy of personal information, including personal health information, in NSW.

It is the responsibility of all NSW Health personnel and their contractors to be aware of and comply with the obligations imposed by the Act.

It is also the responsibility of all NSW Health personnel and their contractors to be aware of and comply with the requirements of the NSW Health Privacy Manual Version 2 (PD2005_593) and the NSW Health Privacy Management Plan (PD2005_554).

These documents list the relevant NSW Health Policy Directives, other NSW Health and government policies and the relevant laws. It is the responsibility of all NSW Health personnel and their contractors to be aware of and comply with the obligations imposed by these policies and laws.

4. Scope

This policy covers security requirements for NSW Health information including electronic personal health information.

“Electronic information” is information that is electronically created, processed, held, maintained and transmitted by NSW Health. It also refers to information held electronically for or on behalf of other government agencies or private entities.

“Personal health information” is personal information which concerns a person/client’s health, medical history or past or future medical treatment. It also includes other personal information collected in the course of providing a health service or information collected in relation to donation of human tissue.

“Personal information” is information or an opinion (including information or an opinion forming part of a database and whether or not recorded in a material form) about an individual whose identity is apparent or can be reasonably be ascertained from the information or opinion.

Any identifiable information is subject to this policy.

This policy applies to all information created, processed, held, maintained or transmitted by the NSW Health information or communication infrastructure. This policy shall apply to all information held for, or on behalf of, other government agencies or private entities.

Information systems refer to any information or communication infrastructure used by NSW Health and all personnel that work with it, including computer hardware and software, to create, process, hold, maintain or transmit electronic information.
For example:

- file, database and communication servers
- computers and/or devices whether connected to a network or stand-alone (notebooks, terminals, tablets, smart phones, storage devices etc.)
- NSW Health mainframes and mid-range computers
- devices used to store or transmit electronic data (USB storage, switches, wireless access points, etc.)
- providers of information services for NSW Health, government agencies or private entities that have been granted access rights to NSW Health information systems.

This policy applies to all employees, contractors and other persons who, in the course of their work, have access to information (including electronic personal health information) in or on behalf of the NSW public health system. This includes but is not limited to:

- providers of health services such as doctors, nurses, case managers, visiting medical officers (VMO’s) etc.
- providers and allied health personnel
- ambulance officers
- administrators, clerical and service personnel
- support staff

- technical, research, scientific and laboratory personnel
- auditors
- interpreters
- volunteers
- students
- consultants
- temporary and contract personnel
- external custodians of information owned by the department.

The policy applies to:

- NSW Health organisations
- non-government organisations receiving funding from the department where compliance is included in the terms of their funding agreement
- private hospitals and day procedures centres treating public patients / clients on a contractual basis, where the contract includes requirements for compliance with NSW Health policies
- personnel of Health Professional Registration Boards (excluding medical, Dental and Pharmacy boards).

Where access is granted to information held by the public health system for research or other purposes, the person or organisation granted access must, under the conditions of access, also be required to comply with the terms of this policy.

Compliance with this policy and all relevant acts and regulations as they relate to information security is mandatory for management, personnel and all persons handling electronic information, whether directly or indirectly involved in client service delivery.

All personnel and organisations referred to above should be aware of their legislative confidentiality obligations and that the breach of those obligations may result in prosecution and the imposition of a penalty or disciplinary actions.

5. Information Security Requirements

The use of information and information systems is an integral part of most NSW Government activities. Electronic information assets are critical in agencies operations and are key element in delivering trustworthy government services. The security threats to information assets are increasing. The government has a duty to safeguard its large information holdings and must provide credible assurance that it is doing so. In 2001 Cabinet recognised these trends and directed that all agencies were to appropriately protect electronic information. In 2006, the document 'People First – A new direction for ICT in NSW' reaffirmed the importance of information security.

In 2012, a new ministerial memorandum M2012-15 (Digital Information Security Policy) was released. This supersedes M2007-04 (Security of Electronic Information), C2001-46 (Security of Electronic Information), M2001-14 (Implementing the Government’s Electronic Information Security Program), C2003-02 (Electronic Information Security – Business Continuity Planning) and C2004-06 (Electronic Information Security – Certification to AS/NZS 7799).

The Government's digital information systems security objectives as stated in the new Ministerial Memorandum (M2012-15) are:

- **Confidentiality** – to uphold authorised restrictions on access to and disclosure of information including personal or proprietary information.
- **Integrity** – to protect information against unauthorised alteration or destruction and prevent successful challenges to its authenticity.
- **Availability** – to provide authorised users with timely and reliable access to information and services.
- **Compliance** – to comply with all applicable legislation, regulations, Cabinet Conventions, policies and contractual obligations requiring information to be available, safeguarded or lawfully used.
- **Assurance** – to provide assurance to Parliament and the people of NSW that information held by the Government is appropriately protected and handled.

Agencies and shared services providers should adopt the following Core Requirements of the Digital Information Security Policy (DIS Policy):

1. Implement an Information Security Management System as set out in the Digital Information Security Policy;
2. Comply with the minimum controls as set out in the Digital Information Security Policy;
3. Certify the ISMS implementation where applicable;
4. Nominate a Senior Responsible Officer to represent the organisation in the Digital Information Security - Community of Practice where applicable; and
5. Provide attestation to compliance with policy if applicable.

To meet the above requirements and provide appropriate assurance, implementation guidance is included as appendix A.

Management must ensure that the implementation of information security is aligned with the organisation’s goals. This will be an important aspect for management to consider as it addresses the requirements specified by the national standards. While these standards specify particular practices to safeguard electronic information, these practices must not be adopted without regard for the organisation’s actual risk profile and business objective(s).

Guidelines should be developed where requirements specified by the standards need to be amended to meet the specific requirements of NSW Health. Not all the controls described in the standard will be relevant to every situation, nor can they take account of local environmental, budgetary or technological constraints, or be present in a form that suits every potential user in an organization.

The risk management approach allows for the tailoring of the controls to the situation. The National Standards AS/NZS ISO 31000 Risk management - Principles and guidelines, (or subsequent versions) should be used in implementing this approach.

6. National Standards

The national standards for an Information Security Management System (ISMS) are:

- AS/NZS ISO/IEC 27001:2006 Information technology – Security techniques – Information security management systems – Requirements; and
- AS/NZS ISO/IEC 27002:2006 Information technology – Security techniques -Code of practice for information security management.

Both have been formally adopted unchanged as Australian & New Zealand standards and the previous standard 17799 has been renumbered as 27002. The standards are reviewed and updated about every 3 years and compliance is always to be to the current editions. Certification is to AS/NZS ISO/IEC 27001 and certifiers must be accredited by an accreditation body authorised by a national government.

The security standards are management standards and there are synergies between information security management and other management standards such as AS/NZS ISO 9001 Quality Management Systems or ISO/IEC 20000 Information technology - Service management (ITIL). It is strongly recommended that agencies that have or are seeking compliance with other management standards reduce their implementation effort by using the same management system infrastructure for compliance with different standards.

7. Roles and Responsibilities

The main objective of NSW Health is to deliver high quality care. The availability of reliable and accurate information is a key factor in the delivery of care. Clearly defined roles and responsibilities assist in the proper protection of the information assets of NSW Health.

Management (CEs or their delegates)
Management commitment to information security is demonstrated by ensuring that:

- this policy and other associated policies are implemented;
- an information security risk management system is established;
- adequate resources are allocated to policy implementation

The CIO NSW Health
The CIO NSW Health is responsible for the management of the information security policy, procedures and guidelines.

Data/Business/Information Owners
The Data or Information Owners have the responsibility for defining the corporate information requirements and data governance policies which include development of standards and requirements for security, retention and disposal of corporate information for their information assets. They are responsible to also manage the risks to their information assets regardless if they have outsourced ICT or are sharing the risks with service providers.

Data Custodians
The Data Custodian has the responsibility for establishing and maintaining an acceptable level of data protection, for managing the disclosure of data, for ensuring that the data is used in accordance with the reasons for which it is collected and that the data is complete, of acceptable quality and is available to authorised users.

System Administrators
System administrators need to know and follow acceptable procedures for granting/revoking access, identifying and resolving known vulnerabilities, and monitoring system access. They are responsible for development of practices and procedures to support the policy and ensure compliance with the security requirements of information owners.

IT Technical and Support Staff
IT Technical and Support Staff are charged with ensuring the correct and secure configuration of systems such as servers, networks, firewalls and routers. Systems developers and maintenance staff are responsible for delivering reliable software. Technical staff should understand the business use and risks associated with the technologies being used so that security solutions match the criticality and sensitive nature of the systems. They are responsible for development of practices and procedures to support the policy and ensure compliance with the security requirements of information owners.

Users

Users of agency electronic information play an important role in overall electronic information security planning and risk management process. The effective participation of users requires a certain culture, as well as education. The culture must be supported by management directives, an education program and demonstrable support for the protection of electronic information. Users must be aware of their responsibilities with regards to Information Security and Privacy. Users have a role in identifying and reporting security concerns and incidents to management for investigation and review.

Third Party Businesses and Organisations, Consumers and Other Agencies

The growing existence of inter-connected networks requires the extension of the ‘boundaries’ of an agency. Agency executive management must ensure that third parties understand Information Security requirements and ensure that adequate security controls are in place in their own environment. All third parties must adhere to NSW Health and agency policy and procedures.

Independent Reviewer/Audit

The role of independent reviewers and auditors is to assess the effectiveness and efficiency of implemented controls, assess whether controls are being adhered to, and to check compliance against policy and legislative requirements. Review and audit reports should be noted by executive management and remedial action taken, if appropriate.

Policy Maintenance

This policy shall be reviewed by the NSW Ministry of Health and their delegates to ensure that it remains relevant and up to date with NSW Health business objectives and accurately reflects any changes in legislation or business practices that affect the security of electronic information including electronic personal health information, either directly or indirectly.

8. Appendix A - Implementation Guidelines

Intention and Principles

Technological advancement has provided significant benefits within Health and NSW Government; it has also equipped malicious users with more advanced means and tools to obtain unauthorised access to information. Any information system usage or implementation may be a target for a range of serious threats, including computer based fraud, espionage, sabotage, vandalism and other forms of systems failure or disaster. This may result in risk of data loss/leakage from accidental/malicious unauthorised access, misuse, misappropriation, modification or destruction of information and information systems that may impact service delivery. Moreover, sharing of information for business reasons, using new applications and inter-connected resources, increases the threat of information theft, loss and exposure to breaches.

Considering all the above threats, NSW Health intends to implement a structured and consistent approach to address information security risks within NSW Health. The intention is that all NSW Health agencies operate a comprehensive information security management system that meets their business-orientated security needs. This system is to comply appropriately with the national standard for such systems. Appropriateness is determined by the risks to the agency's information assets and the potential 'business' implications of those risks. To provide assurance to stakeholders, including partners in government or business, the main part of the Information Security Management System (ISMS) is to address the risks based on priorities.

The principles for implementing information security are:

- Managing risks to information assets is the basis for selecting and operating information security countermeasures and controls;
- Information security countermeasures and controls are implemented and operated as elements of an Information security management system that is planned and controlled through effective management processes; and
- The cost of information security countermeasures and controls must be proportionate to the risks to information assets.

Risks and Threats

An information security risk is the combination of the likelihood and consequences of a potential information security incident or event. Information security risks arise from threats that may affect information assets in a way that adversely impacts information security objectives:

- Threats usually exploit vulnerabilities in information systems and the people that use them;
- Threats may originate internally or externally, they may be accidental or deliberate, malicious or well-meant and have human, technical or environmental sources;
- The motives behind malicious or criminal threats vary widely and will, in part, depend on how information assets can be exploited for unauthorised purposes;
- The potential value of unauthorised use of information is an important consideration and may indicate the likelihood of a threat; and
- Unacceptable information security risks are those that the 'business' cannot tolerate.

The key to managing information security risks in an agency is to understand the agency's information assets, their 'business' significance and active involvement of the information owners in managing security of their information.

An information asset has a 'business' owner, 'business' purpose and 'business' value. Asset value includes both its legitimate value and its value to unauthorised users, as well as its importance to the 'business' and wider consequences of a security incident.

Generally an information security incident could have one or more of the following 'business' consequences:

- Loss of financial or material assets by agency or public - May include losses through theft or fraud, rectification costs, legal liabilities, other unbudgeted costs or lost entitlements. Losses will usually be a consequence of an information integrity failure but confidentiality or availability failures may create opportunities for loss or illegitimate gain.
- Injury or death of public or staff - Could be the result of confidentiality, integrity or availability failures. If the consequences are a direct result of an ICT failure (e.g., in a real-time control system) then that system is 'safety critical' and appropriate methods must be applied to it.
- Inconvenience or distress to public or staff - May be a direct or secondary consequence of an event, e.g., a temporary financial loss may cause inconvenience and distress. Could arise from confidentiality, integrity or availability failures.
- Damage to standing or reputation of the Government, an agency or person, including the confidence or morale of stakeholders in a service or agency. It may be lost through confidentiality, integrity or availability failures. Treatments may include publicity campaigns to rebuild reputation or confidence and these have financial costs.
- Assist an offence or regulatory breech, hinder investigation or enforcement - May directly impact law enforcement or regulatory operations. Crime or regulatory avoidance may threaten confidentiality, integrity and availability elsewhere and have other consequences.
- Degrade the capability to deliver services internally or externally - A loss of operating capability is most likely from loss of information integrity or availability. The period required for a failure to become significant will depend on the nature of the information affected and the extent of operating dependency on it. Loss of capability may also cause regulatory non-compliance, adverse effects on stakeholders and loss of control over activities

Approach

The overall objective of a management system is to ensure that current information security risks are properly identified and effectively and efficiently managed. This emphasises that information security is a management issue and a matter of information and communication technology (ICT) governance, not merely a technical problem. Deploying appropriate technical measures is necessary but insufficient to ensure continuing information security. When identifying possible threats a broad 'business' approach must be taken to the value of an agency's information. This approach must consider at least agency, government and public perspectives.

Identification and assessment of the main risks enables suitable management arrangements and key policies to be established. These provide the information security management framework. Once this framework exists critical risks can be assessed more thoroughly and other risks considered. With management arrangements in place appropriate security measures, including procedures and processes, can be planned, adapted or implemented.

Access Control

Access control is one of the most important countermeasures in ensuring that individuals are restricted to information on a need-to-know basis and protect corporate information from unauthorised access. This concept is known as the principle of least privilege. Controls and standards for logical access should be detailed, comprehensive, and effective.

Access to NSW Health information assets will be granted based on the business need for such access. To maintain effective control over access to information, the various information asset owners should conduct a regular review of access rights.

User registration should be authorised and ensure that unique user identifier is assigned to all users. Passwords used for authentication must be kept secret and should align with appropriate password policies and standards for the agency.

No group or shared credentials and accounts are allowed for interactive login. User ID's should be unique to each user to ensure audit and control over permissions. The information services director or their delegate may make an exception to this under appropriate circumstances.

Users are accountable for actions performed using their user ID's.

The allocation and use of access privileges should be appropriately managed and restricted. Privileges should be assigned following the principle of least privilege access control and approved by the relevant information asset owner.

Backup & Storage Media Handling

Backup of data and information is required to maintain the integrity and availability of information processing and communication services.

A backup/restore strategy and procedures shall be developed for that purpose to ensure that such information is available in line with business requirements.

Storage media should be appropriately protected and managed based on the classification of information contained on that media.

Usage of personal storage media such as external storage devices is in accordance with the Use and Management of Misuse of NSW Health Communications System PD2009_076.

All storage media which contains information classified “”For Official Use Only or Sensitive” or higher should be disposed of securely and safely by, or on behalf of, the asset owner when the media is no longer required. This should be in compliance with the State Records Authority disposal and retention requirements.

Business Continuity Management

All NSW Health agencies should develop a business continuity plan for all the high risk and critical business functions. These plans should be periodically tested and regularly maintained.

Clear Screen and Clear desk

Users should ensure that unattended equipment has appropriate protection. Computer screens should be locked when unattended and users should shut down or logoff the machines when not being used.

Users should maintain clean and secure storage and work areas and ensure sensitive documents are secured appropriately. Sensitive documents and information should not be left unattended.

All documents which are no longer required can be disposed of in a secure fashion. This should be in accordance with State Records Authority and any other disposal regulation or applicable policy.

All non-public documents when printed or scanned should be cleared from printers or scanners, as soon as practical, especially if they are classified as for official use only, sensitive or higer.

Confidentiality Agreements

Confidentiality or Non-Disclosure Agreements (NDA) for protection of “for official use only”, “sensitive” or higher classifications - NSW Health information should be signed before granting access to contractors and third parties.

Cryptographic Controls

Based on the risk profile of information systems appropriate cryptographic controls should be used. Cryptographic controls will be deployed and managed as directed by the regulations governing any such usage.

To maintain the security and integrity of the cryptographic keys and their underlying infrastructure, processes and procedures should be developed and documented to avoid risk exposure to information assets.

Electronic Messaging

Electronic messaging such as email can lead to accidental or deliberate disclosure of information to unauthorised users. For this purpose, the Management and Misuse of NSW Health Communications Systems (PD2009_076) Policy Directive should be adhered to by users of the email system.

Sending information that is classified as ‘sensitive’ or higher to the destinations external to the NSW Health should be encrypted using approved encryption technologies, in accordance with local laws and regulations. Communication standards such as email, FTP, telnet, Mobile SMS, instant messaging and web traffic (HTTP) are not considered secure and should be avoided.

Equipment Security

Only authorised equipment can be connected to NSW Health networks and equipment. This includes mobile devices, modems, PDAs, wireless access points, portable storage devices, CD/DVD burners and printers.

Where possible, equipment should be named and labeled as per a standard naming convention.

Fixed equipment such as servers, networking equipment and desktop computers belonging to NSW Health shall only be removed with proper authorisation. Procedures shall be used to secure equipment used outside of NSW Health premises.

All equipment should be maintained in accordance with the recommended service specification and should be disposed securely when no longer required.

Hardcopy Information

The primary focus of these guidelines is on electronic information. In practice the boundary between hard and softcopy is seldom clear-cut from a security perspective because of transformation between them. However, the inherent characteristics of the different media mean that the risks are different.

Generally, the integrity and confidentiality of hardcopy information is less vulnerable to large-scale loss but the difficulty of maintaining hardcopy 'backups' can make the availability of this type of information more vulnerable to disasters. It is not the intention that agencies review and update the security measures for all their existing hardcopy information. However, improved physical security for electronic information assets will often improve the security of hardcopy information. Further guidance is given in Premier's Circular 2002-69 Labeling Sensitive Information.

Human Resources /Personnel - Security

Recruitment and selection processes for personnel, contractors, vendors and contingent workers will be undertaken to ensure adequate background, reference and criminal record assessments. Adequate induction and ongoing training should be provided taking into account the sensitivity of the position, and the classification of information they have access to.

Documented processes managing the change or termination of employment will be followed.

ICT Operations

Controls shall be introduced in networks to segregate groups of information services, users and information systems based on the sensitivity of the information. NSW Health networks should provide segregation between internal and external networks.

Access to network equipment should be restricted to authorised personnel only.

All changes to the ICT environment should be approved through formal change management practices.

Information Asset

Narrowly defined, electronic information assets are the data and software; owned by, licensed, leased or entrusted to an agency. It may be at rest or in transit within an agency's systems, or being communicated to an external party. An extended definition includes hardware, networks and intangibles such as reputation, goodwill, trust, staff morale and productivity. It may be appropriate to deal with the intangibles as possible consequences of security incidents affecting other information assets.

Each information asset has an owner or custodian within the agency. The ICT group may be the 'owner' of ICT infrastructure. However, business information is 'owned' by business units. These units are responsible for ensuring that the risks to their information assets are realistically assessed and appropriately treated in accordance with Government and agency policies, etc. The appropriate level of management must formally accept any residual risks to information assets.

Acceptable usage of information assets are broadly outlined in Use & Management of Misuse of NSW Health Communications Systems, PD2009_076

Interconnection of business and health information systems

Adequate measures should be developed and documented to ensure only approved and authorised interconnection of the NSW Health information systems with other government agencies and any third parties.

Mobile Computing, Tele-working and Remote Access

The use of mobile computing facilities and devices should be strictly governed and controlled. All the mobile computing devices should be adequately secured utilising technologies such as encryption and pass or PIN codes. Where a device is lost or stolen the relevant Information Services department or equivalent should be notified to ensure at-risk services are suspended immediately.

Mobile users should ensure that assets like tokens/laptops/smart devices and mobile phones are not left unattended and visible in public places such as airports, cafes and the back seats of motor vehicles where the risk of theft is higher. Users working remotely should also consider their environment, and take steps to ensure that equipment and information is appropriately secured from theft or disclosure to unauthorised persons.

Tele-working uses communications technology to enable staff to work remotely from a fixed location outside of their branch site location, also known as Remote Access. Remote access should be appropriately authenticated (use of multi-factor authentication is recommended) and connectivity should be protected by approved controls.

Monitoring and Logging

Access of NSW Health networks and resources shall be granted to only those entities who agree on consent of monitoring. Adequate logging mechanism shall be deployed to record user activities, exceptions, and information security events. Logs should be kept for the appropriate retention period to assist in future audit and access control monitoring. These logs should be protected from any accidental or deliberate modification.

The correct setting of computer clocks is important to ensure the accuracy of audit logs, which may be required for investigations or as evidence in legal or disciplinary cases such as forensic investigations. Systems clocks shall be synchronised for accurate recording to a common time source.

Outsourcing

Agencies that outsource any of their electronic information operations retain ownership of and responsibility for their information assets. These agencies should maintain an inventory of the external/third-party service providers and any agency's ISMSs must include these assets if they are in scope.

Agency policies, etc., are to define clearly the detailed security responsibilities of the agency and of the provider of outsourced services affecting the agency's information assets. These will be reflected in contracts and service level agreements with service providers, including mechanisms to ensure they can be modified to reflect changing risks. The goal is to ensure there are no gaps or ambiguities between the ISMSs of the two parties.

Regular reviews of the outsourced services and operations shall be conducted to identify the changes or improvements to the provision of services. Such reviews should also assess ongoing access requirements and compliance to the NSW Health policies.

Generally, agencies are to require the certification of outsourced service providers' ISMS's to the national standard.

Agencies that have outsourced will still require their own compliant and certified ISMS, even when they have no residual 'insourced' ICT. Subject to risk assessment, the outsourcing agency's ISMS Statement of Applicability will focus on the non-technical aspects of their information security environment. This will ensure that the agency has effective measures for the control of their information assets and the use of assets provided by the outsourcer.

Small agencies that function as units of larger ones or are supported by secretariats or staff from larger agencies should be treated as part of the larger agency for information security compliance and certification purposes. Their inclusion should be noted in the larger agency's Statement of Applicability.

Physical Security

NSW Health agencies should ensure adequate physical security is applied on all information processing facilities. The selection and design of information processing premises should take into account the possibility of damage from fire, flood, explosion, accidents, malicious intent, and other forms of natural or man-made disasters.

In addition, all Health agencies should identify and maintain an inventory of physical locations/facilities especially where business critical/sensitive assets are hosted. Delivery and loading areas shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorised access.

Access to sensitive information and information processing locations/facilities is restricted to authorised persons only. An audit trail of access should be maintained especially when access to facilities where sensitive information is located.

Protection against Malicious code including Mobile Code

Software and information processing facilities are vulnerable to the introduction of malicious software. Appropriate controls should be implemented to detect and prevent the introduction of malicious software, such as computer, viruses, worms, Trojan horses, root-kits, spyware, and other malware. Users must not disable or interfere with these controls.

Publicly Available Electronic Information

Release of electronic information to the public or service provider should be approved by the relevant branch authority and/or Communications Department.

Reporting Security Incidents & Managing Contacts

To reduce the business consequences and to take appropriate action against all security concerns and incidents should be reported to senior management. Consistent and repeatable processes should be adopted to address security weaknesses and events across NSW Health.

The health agencies should maintain contacts with authorities and special interest groups for liaison on operational issues. Examples of some authorities and interest groups are;

- Fire and Rescue Department
- Law Enforcement authorities
- NSW Ministry of Police and Emergency Services
- State Emergency Services (SES)
- Telecommunications Service Providers
- Electricity / Energy Service Providers

- Internet Service Providers
- Digital Information Security Community of Practice
- AUSCERT
- Defense Signals Directorate
- Specialist industry forums and groups

Separation of Development, Test and Operational Facilities

The level of separation between production, testing and development environments needs to be considered to prevent operational impact to services. Testing and development environments should be separated from production (operational) facilities.

Use of production data in test and development environments should be carefully controlled, and where possible, sensitive information should be removed before being utilised for testing purposes.

Security Requirements in Systems and Applications

The design and/or implementation of new applications and systems should take into account the security requirements and objectives of the agency. These requirements should include consideration of the classification of the information to be maintained or managed by these systems or applications.

Requirements should also take in to account information retention and business continuity requirements.

Changes to applications and systems should also take into consideration the information security requirements.

Software licensing and use

Only authorised software should be used. Any exceptions should be authorised from appropriate Information Services Director or their delegate. All software should be used in accordance with specified license or copyright terms and conditions. Unlicensed software shall not be installed for any reason.

Technical Vulnerability Management

Sensitive information systems should be subject to periodic vulnerability assessment. Adequate assessment and penetration testing processes should be used to identify the level of risk exposure for other Information systems due to these vulnerabilities. Vulnerabilities and system patches should be prioritised for remediation commensurate with the risk to the NSW agency's information systems.

Technical audit and assessments reports should be considered sensitive and protected to prevent any possible misuse or exploit.

Time Scale and Resources

Agencies are to achieve the Government's information security objectives as soon as possible. Progress will be monitored through a security status framework. Achievement of the objectives is marked by appropriate certified compliance with the standards and continuance of certification.

Information security, like physical security, is a routine function in which all staff has some role. Agencies are to act economically by making maximum use of their internal resources. Training may be necessary in some agencies. Agencies are also strongly encouraged to share security knowledge and resources. In some agencies external resources may be needed to advise, mentor inexperienced security staff and provide expert review of risk assessments and security plans.

Online Financial Transaction

All financial transactions carried out in the public domain or network should deploy the APRA and PCI-DSS recommended controls to protect the systems from fraudulent activity and unauthorised disclosures and modifications. This is in accordance with current regulatory compliance standards