

Electronic Information Security Policy - NSW Health

Document Number PD2008_052

Publication date 15-Sep-2008

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 M2007-04 (Security of Electronic Information). New international and Australian standards are now applicable. 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 [PD2005_314]

Author Branch Strategic Information Management

Branch contact Mark Adler 9391 9885

Applies to Area Health Services/Chief Executive Governed Statutory Health Corporation, Board Governed Statutory Health Corporations, Affiliated Health Organisations - Non Declared, Affiliated Health Organisations - Declared, Public Health System Support Division, NSW Ambulance Service, NSW Dept of Health

Audience Chief Information Officers, Directors of Corporate Services

Distributed to Public Health System, NSW Ambulance Service, NSW Department of Health

Review date 15-Sep-2013

File No. 00/5283

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This Policy Directive may be varied, withdrawn or replaced at any time.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.

ELECTRONIC INFORMATION SECURITY POLICY
Version: 2.0

Table of Contents

1. INTRODUCTION..... 2

2. SECURITY POLICY STATEMENT..... 2

3. PRIVACY STATEMENT 3

4. SCOPE 3

5. INFORMATION SECURITY REQUIREMENTS 5

6. NATIONAL STANDARDS 6

7. ROLES AND RESPONSIBILITIES..... 6

APPENDIX - IMPLEMENTATION GUIDELINES 8

Title: Electronic Information Security Policy – (Version 2)

1. Introduction

This document is Version 2 of the “NSW Health Electronic 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.

Publication of Version 2 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 M2007-04;
- 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).

2. Security Policy Statement

NSW Health¹ is committed to the provision of appropriate levels of security across all of its information systems. Personal health information systems 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.
- the implementation of information security controls must not impact the timely provision of those services.
- 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 will be classified for the purposes of determining the level of security required.
- 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.

¹ In the context of this document the term NSW Health includes all NSW Health organisations. The NSW Health organisation are: Area Health Services (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 Health Support Services), Dental Schools and Clinics, NSW Ambulance Service, and the NSW Department of Health.

Title: Electronic Information Security Policy – (Version 2)

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, or 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 opinion (including information or an opinion forming part of a data base 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 electronic information created, processed, held, maintained or transmitted by the NSW Health information or communication infrastructure. This policy shall apply to all electronic 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 within it, including computer hardware and software, to create, process, hold, maintain or transmit electronic information.

This includes:

- file, database and communication servers
- computers connected to the Wide Area Network (WAN), local area network (LAN) or stand-alone
- NSW Health mainframes and mid-range computers
- devices used to store or transmit electronic data
- providers of information services for NSW Health, government agencies or

Title: Electronic Information Security Policy – (Version 2)

- private entities that have been granted access rights to NSW Health information technology 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
- 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 there is access granted to information held by public health system for research or other purposes, the person or organisation granted access should, 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 organizations 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.

Title: Electronic Information Security Policy – (Version 2)

5. Information Security Requirements

The use of information and information systems is an integral part of most NSW Government activities. Electronic information assets are increasingly critical in agencies' operations and a 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 'People First – A new direction for ICT in NSW' reaffirmed the importance of information security.

In 2007 a new Ministerial Memorandum (M2007-04) was released This supersedes 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 electronic information security objectives as stated in the new Ministerial Memorandum are:

- 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;
- Confidentiality. To uphold authorised restrictions on access to and disclosure of information including safeguarding personal or proprietary information;
- Compliance. To comply with all statutes, regulations, Cabinet Conventions, policies and contractual obligations requiring information to be available, safeguarded or lawfully used; and
- Assurance. To provide assurance to Parliament and the people of New South Wales that information held by the Government is appropriately secure.

Agencies are to act as follows in achieving these objectives:

- Policy and Organisation. Establish policies and practices, an appropriate management structure and responsibilities up to executive level for information security management;
- Risk. Identify information assets and use a risk management process to reduce the likelihood and or consequences of security incidents to an appropriate and acceptable level;
- Appropriateness. Ensure the totality of security measures is commensurate with the significance, value of and risks to their information assets;
- Compliance. Establish and maintain an agency wide Information Security Management System that complies with the national standard and covers all electronic information; and
- Certification. Gain and maintain certified compliance to the new national standards of the main part(s) of their Information Security Management System by an accredited certifier. Exemptions from this requirement may be granted based on the risks to an agency's information assets. Further details of what constitutes the main parts of the organisation's Information Security Management System (ISMS) are given in the appended Implementation Guidelines.

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

Title: Electronic Information Security Policy – (Version 2)

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 Standards Australia document "HB231:2004, Information Security Risk Management Guidelines" (or subsequent versions) should be used in implementing this approach.

6. National Standards

The new 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 electronic information security policy and guidelines.

Data Custodians

Title: *Electronic Information Security Policy – (Version 2)*

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 and 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.

IT Technical and Support Staff

IT Technical staff are charged with ensuring the correct 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.

Users

Users of agency electronic information play an important role in overall electronic information security plan 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.

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.

Independent Reviewer/Audit

The independent reviewer and auditors role 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 Review

This policy shall be reviewed at least annually by the NSW Department of Health Strategic Information Management Branch which shall 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.

Professor Debora Picone AM
Director-General

Implementation Guidelines

The intention is that all agencies operate a comprehensive electronic information security management system that meets their business oriented 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 their 'business' implications. To provide assurance to stakeholders, including partners in electronic government or business, the main part of the Information Security Management System (ISMS) is to maintain certified compliance with the national standard.

Principles

The three principles for implementing electronic information security are:

- Managing risks to information assets is the basis for selecting and operating information security measures;
- Information security measures are implemented and operated as elements of an information security management system that is planned and controlled through effective management processes; and
- The sum of information security measures 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 an information security incident. 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 significance includes both its legitimate value and its value to unauthorised users as well as its importance to the 'business' and 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.

Title: Electronic Information Security Policy – (Version 2)

- 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 (eg 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, eg 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 Includes the confidence or morale of stakeholders in a service or agency. It may be lost by 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 breach, 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

The 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 27002:2008** 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.

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.

Title: Electronic Information Security Policy – (Version 2)

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.

Scope of Compliance and its Certification

Most of the security controls in the current standards will be applicable to some extent. However, in practice some controls will only be marginally relevant or treating acceptable residual risks. These controls should be given low priority and compliant information security management can be achieved without applying them. The standard is not a 'checklist' requiring a 'tick' in every box.

The cost of any security measures must be less than the cost of the consequences of security incidents taking account of their likelihood. This means that some standard security controls may not be used but the agency will still have a suitably comprehensive, compliant and partially certifiable ISMS. Nevertheless, all risks must be periodically reviewed and if they become unacceptable they must be treated with additional or updated security measures.

Suitably comprehensive compliance does not mean comprehensive certification. The purpose of certification is similar to having independently audited financial accounts. It gives assurance to the stakeholders that information security risks are being properly managed. Full certification does not always provide value for money in large agencies with many local offices if each requires auditing. However, an excessively narrow certification rarely provides value for money or an appropriate degree of assurance. Certification should focus on the main part of the business critical ISMS.

When deciding the business critical part of an ISMS the following approach is to be used:

- The certification covers the agency's most important information assets and those most at risk in terms of the likelihood of a security incident and its consequences; and
- The certification covers significant information assets including those:
 - about identifiable members of the public;
 - with sensitive information about identifiable employees;
 - where a security failure could:
 - ◇ result in loss of life or injury
 - ◇ result in significant fraud;
 - ◇ affect the delivery of major services;
 - ◇ result in significant damage to government reputation;
 - ◇ undermine regulatory or law enforcement activity;
 - where electronic information is received from or provided to another agency; or
 - where electronic information is X-IN-CONFIDENCE, PROTECTED, HIGHLY PROTECTED (Premier's Circular 2002-69) or has a national security classification of RESTRICTED or higher.

The certified ISMS should include security policies, procedures and processes that are used throughout the agency. This does not mean that all parts of the agency using these

Title: *Electronic Information Security Policy – (Version 2)*

have to be within the certified ISMA. Certification of policies, etc, in an ISMS gives confidence that they are generally satisfactory.

Uncertified parts of an information security management system are to be periodically audited for compliance with the agency's policies and procedures by internal or external auditors. Results are to be formally reported to the agency's board or equivalent executive group if there is no board.

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' makes their availability 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 information assets will often improve the security of hardcopy information. Further guidance is given in Premier's Circular 2002-69 Labelling Sensitive Information.

Information Asset

Narrowly defined electronic information assets are the data and software owned by, licensed 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.

Outsourcing

Agencies that outsource any of their electronic information operations retain ownership of and responsibility for their information assets. These agencies' Information Security Management Systems must include these assets. 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 Information Security Management Systems of the two parties.

Generally, agencies are to require the certification of outsource service providers' ISMS to the national standard. This certification provides assurance to the agency about the security of their assets entrusted to the outsourcer and hence to the agency's stakeholders. Exceptionally this may be unnecessary where the agency's information assets are not at unacceptable risk from a security incident affecting the outsourcer's capabilities; for example agency operated encryption on outsourced communications bearers.

Title: Electronic Information Security Policy – (Version 2)

Outsourcing agencies 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 their security policies and organisation, compliance with legal obligations, asset management, staff behaviour, physical security, security incident management and business continuity. 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.

Timescale 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 have 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.

Exemption

Agencies without significant information assets may apply for an exemption from the requirement to obtain and maintain certified compliance. Such agencies will still need to achieve appropriate uncertified compliance. Details will be promulgated separately.

In the framework of the significant information assets outlined above, exemptions will consider the extent and sensitivity of individual records, the consequences of significant fraud or altered information, of compromise to regulatory or law enforcement activities, service delivery failures, the impact of a security failure on government reputation or if the agency exchanges significant electronic information with another agency.

For very small agencies resource limitations will also be considered. Such limitations would make an average of 3 or 4 certification auditor days per year unaffordable.

Reporting

Agencies are to report their security status at least annually to the Government Chief Information Office. This reporting will be online and be based on a security status framework. Details will be promulgated separately.

NSW Department of Commerce guidelines

Guidelines for the implementation of the above requirements are given in current the document called "*Information Security Guidelines*"² published by the Government Chief Information Office. This is available via the NSW Department of Commerce website (www.commerce.nsw.gov.au). These guidelines should be followed by Health organisations.

² The title of the document is "GCIO Guidelines – Information Security Guidelines" (Issue 6, Feb 2007, ISBN: 0734743904).