NSW Government
Digital Information Security Policy

Version: 1.0
Date: November 2012

CONTENTS

PART 1 PRELIMINARY

1.1 Scope

This Policy establishes the **digital information** security requirements for the NSW public sector, including the requirement to have an Information Security Management System (ISMS) that takes into account a minimum set of controls, and requirements relating to certification, attestation and the establishment of the Digital Information Security Community of Practice.

This policy does not specifically cover the security of hardcopy information; however, the objectives of this policy apply equally to information in any format.

1.2 Application

This policy applies to all NSW Government Departments, Statutory Bodies and Shared Service Providers.

In accordance with Premier's Memorandum *M1999-19 Applicability of Memoranda and Circulars to State Owned Corporations*, this policy does not apply to State Owned Corporations; however, it is commended for adoption.

1.3 Objectives

This policy aims to ensure that the following digital information and digital information systems security objectives are achieved by the NSW Government:

- **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.

•

PART 2 CORE REQUIREMENTS

Core Requirement 1—Information Security Management System

All NSW Government Departments, Statutory Bodies and Shared Service Providers must have an Information Security Management System (ISMS) based on a comprehensive assessment of the risk to digital information and digital information systems. The ISMS must appropriately address all identified risks and must take account of:

1. *NSW Treasury Policy & Guidelines Paper TPP09-05 - Internal Audit and Risk Management Policy for the NSW Public Sector*
2. *AS/NZS ISO 31000 Risk management - Principles and guidelines*
3. *AS/NZS ISO/IEC 27001 Information technology - Security techniques - Information security management systems – Requirements* and *AS/NZS ISO/IEC 27002 Information technology - Security techniques - Code of practice for information security management* and related Standards

All Departments and Statutory Bodies must also ensure that any Public Sector Agency under its control with a risk profile sufficient to warrant an independent ISMS undertakes to develop an ISMS in accordance with the Core Requirements of this policy.

The ISMS must be reviewed at least annually or when changes to risk are identified.

Core Requirement 2—Compliance with Minimum Controls

In developing the ISMS, all controls from *AS/NZS ISO/IEC 27002 Information technology - Security techniques - Code of practice for information security management* must be considered.

As a minimum, the ISMS must contain measures that address the risks associated with the set of Security Categories in Table 1, taking into account the controls identified from *AS/NZS ISO/IEC 27002*.

Table 1: Digital Information and Digital Information Systems Security Minimum Controls

Security Category	AS/NZS ISO/IEC 27002 Control(s)
1. Governance	
Information Security Management Systems must include the following governance arrangements: o an Information Security Policy; and o a designated individual (Senior Responsible Officer) responsible for digital security. Senior management must provide direction and support for digital information and digital information systems security in accordance with business requirements and relevant laws and regulations.	5.1.1 5.1.2 6.1.1 6.1.2 6.1.3
2. Information security systems independent review	
Information Security Management Systems must be reviewed in accordance	6.1.8

Security Category	AS/NZS ISO/IEC 27002 Control(s)
with the level of risk to digital information and digital information systems. This may be as part of an audit process.	
3. Information classification	
All digital information must be classified to ensure it receives an appropriate level of protection. In classifying information, regard must be given to obligations imposed by relevant laws and regulations, in particular the *Privacy and Personal Information Protection Act 1998* and *Government Information (Public Access) Act 2009*.	7.2.1 7.2.2
4. Controlling access to information systems	
Access to digital information and digital information systems must be monitored and controlled.	10.8.4 10.9.1 10.9.2
5. Processing, handling, integrity and storage of information and documentation	
Controls must be in place to prevent unauthorised disclosure, modification, removal or destruction of digital information.	10.7.1 10.7.2 10.9.1 10.9.3
6. Purchasing/maintaining information systems	
Security must be an integral consideration in information systems purchasing and maintenance.	6.1.4 12.1.1
7. Controlling relationships with external parties	
The security of digital information and digital information systems accessed, processed, communicated to, or managed by external parties must be controlled. The security of digital information and software exchanged with any external entity must be maintained.	6.1.5 6.2.1 6.2.2 6.2.3 10.8.1 10.8.2
8. Business processes and continuity	
Controls must be in place to counteract interruptions to business activities and to protect critical business processes from the effects of major failures of digital information systems or disasters. The timely resumption of business processes in the event of a major failure must be ensured.	10.8.5 14.1.1 14.1.4
9. Reporting information security events/incidents/near misses/weaknesses	
Internal processes must be in place for the communication of digital information security events, incidents, near misses and weaknesses associated with digital information systems, and timely corrective action must be taken.	6.1.6 13.1.1
10. Collaboration and information sharing	
A collaborative approach to information security, facilitated by the sharing of information security experience and knowledge, must be maintained.	6.1.7

Core Requirement 3—Certified Compliance with *AS/NZS ISO/IEC 27001*

In addition to demonstrating compliance with Core Requirement 1 and Core Requirement 2, certified compliance with *AS/NZS ISO/IEC 27001 Information technology - Security techniques - Information security management systems - Requirements* must be maintained by:

1. All Shared Service Providers; and
2. Any Department or Statutory Body, or part thereof, or Public Sector Agency under the control of a Department or Statutory Body whose risk profile is sufficient to make certification necessary.

Certification must be continuously maintained through audits conducted by an Accredited Third Party.

Core Requirement 4—Community of Practice

Digital information security events, incidents and near misses that pose a threat across the public sector must be disseminated through the Digital Information Security Community of Practice in a time and manner appropriate to the nature and magnitude of the threat.

All Departments, Statutory Bodies and Shared Service Providers must maintain an up-to-date listing of their Senior Responsible Officer with the Digital Information Security Community of Practice Register. The listing must include the Senior Responsible Officer's name, position, email address, and work and mobile telephone numbers.

Change of Senior Responsible Officer, or a change of details, must be communicated within ten working days.

Core Requirement 5—Compliance Attestation

Departments and Statutory Bodies – Annual Attestation

Each Department and Statutory Body must attest annually to the adequacy of its digital information and information systems security. Attestation must be presented in the Annual Reports of all Departments and Statutory Bodies.

Attestation must be provided in accordance with ANNEX A of this policy.

Shared Service Providers – Annual Attestation & Evidence of Certification

Each Shared Service Provider must attest annually to the adequacy of its digital information and information systems security and provide evidence in writing of certification by an Accredited Third Party. Attestation and evidence of certification must be sent to the NSW Government ICT Board on or before 30 June each year, beginning in 2014.

Attestation and evidence of certification must be provided in accordance with ANNEX B of this policy.

PART 3 IMPLEMENTATION

All NSW Government Departments, Statutory Bodies and Shared Service Providers are expected to commence implementation of this policy by 31 August 2012 and to have achieved full compliance by 31 December 2013.

All Departments, Statutory Bodies and Shared Service Providers must comply with the implementation actions in this Part.

3.1 Implementation Progress Report

All Departments, Statutory Bodies and Shared Service Providers are required to report progress towards implementation on or before 31 July 2013 AND on or before 31 January 2014 in accordance with ANNEX C of this policy.

3.2 Nomination to the Community of Practice

All Departments, Statutory Bodies and Shared Service Providers must communicate the details of their Senior Responsible Officer to the Digital Information Security Community of Practice Register in writing by 31 January 2013. Nominations should be sent to:

Digital Information Security Community of Practice Register
c/- ICT Policy
Department of Finance & Services
Level 17, McKell Building
2-24 Rawson Place
SYDNEY NSW 2000
E: informationsecurity@services.nsw.gov.au

3.3 Community of Practice Charter

It is expected that meeting of the Digital Information Security Community of Practice will be convened by December 2012 and a Charter of Operation will be adopted. The Digital Information Security Community of Practice Charter will include the structure, objectives and outcomes of the Community, reporting requirements and frequency of meetings.

3.4 Information Classification

In the first quarter of 2013 the NSW Government will begin transitioning to a new system for classifying information that provides for classification consistent with the *Australian Government security classification system*. The new system will be published by a Premier's Circular superseding Premier's Circular *C2002-69 Labelling Sensitive Information*, and will include notes and guidance to assist agencies to transition to the new system.

The Community of Practice will be leveraged to assist with implementation of the new system for classifying information.

All information classified on or after 1 January 2014 will be required to be classified in a manner consistent with the *Australian Government security classification system*.

PART 4 NOTES AND GUIDANCE

4.1 Definitions

Unless otherwise stated, the following definitions apply in this document:

Accredited Third Party: certifiers accredited by an accreditation body authorised by a national government in accordance with *ISO/IEC 27006 Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems*.

Department: any entity designated a Department under the *Public Finance and Audit Act 1983*.

Department Head: as designated in Schedule 3 of the *Public Finance and Audit Act 1983*.

Digital Information: the data owned by, licensed or entrusted to an agency. It may be at rest or in transit within the systems used by an agency, or being communicated to an external party.

Digital Information Systems: software, hardware and networks used to store, transport, manage and access digital information.

Information Security Event: an identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant.

Information Security Incident: a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security

Information Security Management System: as defined by *AS/NZS ISO/IEC 27001 Information technology - Security techniques - Information security management systems - Requirements*.

Public Sector Agencies: all agencies of the NSW public sector as defined by the *Public Sector Employment and Management Act 2002*.

Shared Service Provider: any entity that provides functions that are leveraged across multiple agencies or Departments. Functions may include:

- business shared services relating to operating or frontline services; and/or
- corporate shared services relating to services within corporate functions, such as finance and human resource management.

A reference to Shared Service Providers is a reference to both internal and external shared service providers.

State Owned Corporation: any entity designated a State Owned Corporation under the *State Owned Corporations Act 1989*.

Statutory Body: any entity designated a Statutory Body under the *Public Finance and Audit Act 1983*.

4.2 Referenced Documents

The following documents are referenced in this policy:

Legislation, Policies and Guidelines

- *Australian Government Security Classification System (2011)*
- *Government Information (Public Access) Act 2009*
- *M1999-19 Applicability of Memoranda and Circulars to State Owned Corporations*
- *M2007-04 Security of Electronic Information*
- *NSW Auditor-General's Report: Performance Audit: Electronic Information Security (2010)*
- *NSW Government ICT Strategy 2012*
- *NSW Treasury Policy & Guidelines Paper TPP09-05 – Internal Audit and Risk Management Policy for the NSW Public Sector*
- *Privacy and Personal Information Protection Act 1998*
- *State Owned Corporations Act 1989*
- *Australian Accounting Standards*

Standards

- *AS/NZS ISO/IEC 27001 Information technology - Security techniques - Information security management systems - Requirements*
- *AS/NZS ISO/IEC 27002 Information technology - Security techniques - Code of practice for information security management*
- *AS/NZS ISO 31000 Risk management - Principles and guidelines*

4.3 Related Policies and Legislation

- *Australian Government Cyber Security Strategy*
- *Defence Signals Directorate: Australian Government Information Security Manual*
- Defence Signals Directorate: *Strategies to Mitigate Targeted Cyber Intrusions*
- *Defence Signals Directorate: Top Four Mitigation Strategies to Protect Your ICT System*
- *Federal Attorney-General's Department Protective Security Framework*
- *Health Records and Information Privacy Act 2002*
- *Premier's Circular C2002-69 Guide to Labelling Sensitive Information*
- *State Records Act 1998*

4.4 Core Requirements – Notes and Guidance

The following provides guidance on complying with the Core Requirements of this policy.

Core Requirement 1 Notes and Guidance

Senior Responsible Officer

The Senior Responsible Officer should be the individual with carriage of the ISMS or a person delegated by them. The Senior Responsible Officer should have visibility of all digital information and digital information systems management and policy within the organisation,

and should have the requisite knowledge and experience to develop, implement and manage the ISMS.

The Senior Responsible Officer should have the authority to represent the organisation in the Community of Practice.

In smaller organisations, the Senior Responsible Officer role may be fulfilled by the chief information officer, head of information technology or similar as part of their portfolio of responsibilities.

Control of a Public Sector Agency

For the purpose of Core Requirement 1, 'control' of a Public Sector Agency is consistent with the definition provided in the *Australian Accounting Standards*.

Departments and Statutory Bodies that do not manage their own digital information or digital information systems

It may be appropriate for Departments or Statutory Bodies that do not store or directly manage their own digital information and digital information systems to share some risk with a service provider. Where this is the case, the risk shared with the service provider should be explicitly stated in the ISMS. Ownership of and responsibility for the digital information and digital information systems that are the subject of the shared risk should be clearly outlined in the ISMS and in any contractual agreements with the service provider.

Where risk is shared with a service provider, the ISMS should concentrate on Minimum Control 7, *Controlling relationships with external parties*.

Departments or Statutory Bodies that share risk with a service provider must be satisfied that the service provider has sufficient security controls in place to adequately protect the digital information and information systems of the Department or Statutory Body in accordance with this policy and statutory obligations.

Departments or Statutory Bodies that fall into this category are still required to satisfy Core Requirement 4—Compliance Attestation.

Departments and Statutory Bodies with technologically autonomous sub-agencies

The ISMS of a Department or Statutory Body require a sub-agency of that Department or Statutory Body to have an independent ISMS.

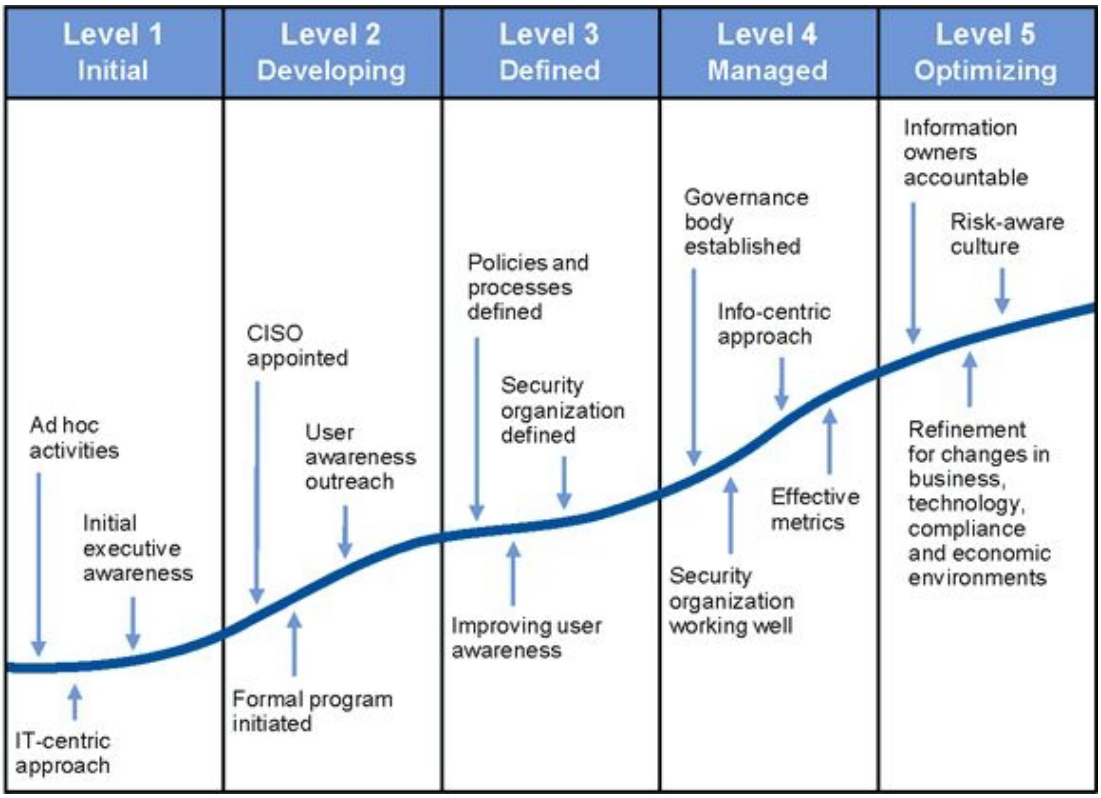
In this case, the provision requiring the sub-agency to develop an independent ISMS is, for the purpose of the Department's or Statutory Body's digital information security, an adequate control to mitigate the risk to the digital information assets and systems of the sub-agency

The Department or Statutory Body need not maintain control or visibility over a sub-agency's independent ISMS to attest to its digital information security. It is sufficient that the Department or Statutory Body is satisfied that an ISMS has been implemented.

Reviewing the ISMS

When planning and operating the ISMS, Departments, Statutory Bodies and Shared Service Providers are encouraged to self-assess the maturity of their security management using the Gartner *ITScore for Information Security*. This tool provides an objective estimate of how effectively information security is integrated into business and ICT management processes. Figure 1 shows key milestones for each maturity level. The resulting score can be further used to measure improvements achieved through the implementation of the ISMS.

Figure 1: ITScore Maturity Levels for Information Security



Core Requirement 2 Notes and Guidance

Minimum Controls

In addition to the Security Categories and minimum controls listed in Table 1, the ISMS should consider the adoption of all controls from *AS/NZS ISO/IEC 27002 Information technology - Security techniques - Code of practice for information security management* based on a thorough assessment of the risk to digital information assets and systems.

Information security systems independent review

The requirement for independent review may be satisfied by certified compliance with *AS/NZS ISO/IEC 27001 Information technology - Security techniques - Information security management systems - Requirements* in accordance with Core Requirement 3.

Independent review may also be part of an internal audit process. Where this is the case, auditors should understand the digital information and digital information systems security environment; however, they should not have contributed directly to the development of the ISMS.

Additionally, independent review may be part of a peer review process or outsourced to external contractors, who provide audit services without the need for certification and need not be accredited to provide the certification.

In determining the appropriate method of independent review, the sensitivity and business criticality of the information assets covered by the ISMS and the level of risk to information and information systems should be taken into account.

Core Requirement 3 Notes and Guidance

Shared Service Providers

For the purposes of this policy, as at 30 June 2012 NSW Government Shared Service Providers are as in Table 2.

Table 2: NSW Government Shared Service Providers as at 30 June 2012

Internal	External
Attorney General and Justice Shared Services	ServiceFirst
Transport Shared Services	BusinessLink
Education Shared Services	
Health Support Services	

When certification is required under Core Requirement 3

In assessing a risk profile for the purpose of determining whether certification is necessary, the sensitivity of the digital information and the risk to digital information and digital information systems covered by an ISMS should be taken into account.

A risk profile sufficient to make certification necessary under the second head of Core Requirement 3 may be indicated by the following:

- Where an ISMS covers digital information assets that contain information about identifiable members of the public;
- Where an ISMS covers digital information assets that contain 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 digital information is received from or provided to another agency; or
- Where digital information is SENSITIVE, PROTECTED, CONFIDENTIAL, SECRET or TOP SECRET.

It is the expectation of the NSW Government that entities whose digital information assets contain particularly sensitive information, or whose assets and systems are at a particularly high risk of a security event, will identify themselves as requiring full compliance with the Standard, and undertake to achieve certification by an Accredited Third Party.

Determining what should be certified

Certification should focus on the main part of the business critical ISMS. The certification should cover the agency's most important information assets and those most at risk in terms of the likelihood of a security event and its consequences.

Core Requirement 4 Notes and Guidance

Digital Information Security Community of Practice

The Digital Information Security Community of Practice will comprise Senior Responsible Officers from all Departments, Statutory Bodies and Shared Service Providers. It will

facilitate implementation of the policy, share best practice and disseminate information on security risks that pose a threat across the NSW public sector.

Digital Information Security Community of Practice Register

A register of Senior Responsible Officers (the Digital Information Security Community of Practice Register) will be maintained by the Department of Finance & Services. Change of Senior Responsible Officer, or a change of details, should be sent to:

Digital Information Security Community of Practice Register
c/- ICT Policy
Department of Finance & Services
Level 17, McKell Building
2-24 Rawson Place
SYDNEY NSW 2000
E: informationsecurity@services.nsw.gov.au

Dissemination of events, incidents and near misses

In determining the nature and magnitude of a threat, and the appropriate time and manner for its dissemination, regard should be given to the following:

- Whether the threat pertains to information about identifiable members of the public;
- Whether the threat pertains to sensitive information about identifiable employees;
- Whether the realisation of the threat 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;
- Whether the information is/was received from or provided to another agency; and
- Whether the information is SENSITIVE, PROTECTED, CONFIDENTIAL, SECRET or TOP SECRET.

Core Requirement 5 Notes and Guidance

Scope of Attestation – Departments and Statutory Bodies

The scope of attestation extends as far as the scope of the annual reporting requirements for the Department or Statutory Body in accordance with the *Public Finance and Audit Act 1983*. Those agencies and business units whose financial records are contained in the annual report of a Department or Statutory Body should be covered by the ISMS of the Department or Statutory Body and are included in the scope of the attestation.

It is noted that this is the same scope as the attestation required by Treasury Policy TPP09-05 Internal Audit and Risk Management Policy for the NSW Public Sector.

4.5 Timetable of Key Implementation Dates

Table 3: Timetable of Key Implementation Dates

Date	Deliverable	Affected Entities
31 January 2013	Nomination of Senior Responsible Officer provided to the Digital Information Security Community of Practice Register	All Departments, Statutory Bodies and Shared Service Providers
31 July 2013	First Implementation Progress Report provided to the NSW Government ICT Board	All Departments, Statutory Bodies and Shared Service Providers
31 January 2014	Second Implementation Progress Report provided to the NSW Government ICT Board	All Departments, Statutory Bodies and Shared Service Providers
1 January 2014	All information must be classified in a manner consistent with the *Australian Government security classification system*	All Departments, Statutory Bodies and Shared Service Providers
30 June each year from 2014 onwards	First Annual Attestation and Evidence of Certification provided to the NSW Government ICT Board	All Shared Service Providers
Each Annual Reporting Period from 2013-14 onwards	Annual Attestation Statement to appear in Annual Report	All Departments and Statutory Bodies

4.6 Enquiries

General inquiries concerning this document should initially be directed to:

Director, Information
ICT Policy
Department of Finance & Services
Level 17, McKell Building
2-24 Rawson Place
SYDNEY NSW 2000
E: informationsecurity@services.nsw.gov.au

PART 5 BACKGROUND TO THE POLICY

Digital information and digital information systems are an integral part of most NSW Government activities. Digital information assets and the systems that house them are increasingly critical in agency operations and a key element in delivering trustworthy and reliable government services.

Formerly, the Government approach to digital information and digital information systems security in NSW was defined by Premier's Memorandum *M2007-04 Security of Electronic Information*, which required public sector agencies to maintain certified compliance with *AS/NZS ISO/IEC 27001 Information technology - Security techniques - Information security management systems - Requirements*.

In 2010 the NSW Auditor General reported on agencies' implementation of the policy outlined under M2007-04. Among other things, the report found that "The Government cannot say with any certainty whether agencies have implemented its policy. As a result, the Government does now know how well agencies are securing sensitive personal information," and that "Progress toward compliance and certification has not been effectively monitored."

In July 2011 the ICT Board approved the development and circulation of a discussion paper on proposed reforms to information security. All agencies were given the opportunity to comment on the paper and in November 2011 the ICT Leadership group considered the responses as part of the development of the *NSW Government ICT Strategy 2012*, which was released in May 2012.

A revised electronic information security policy is a key element of the ICT Strategy, which commits to implementing electronic information security in a consistent manner across the NSW public sector.

Between March and June 2012 a working group comprising both public and private sector participants with experience in the area of electronic information security met to refine and agree the key elements of the policy for approval by the ICT Board. This policy is a product of that working group process.

This policy supersedes *M2007-04 Security of Electronic Information*. In accordance with the *NSW Government ICT Strategy 2012*, all agencies are to have completed implementation of this policy by 1 December 2013.

ANNEX A ANNUAL ATTESTATION

A.1 Annual Attestation Requirements

Each NSW Government Department and Statutory Body must include a Digital Information Security Annual Attestation Statement in its Annual Report under the section dealing with risk management and insurance activities.

From 2013-14 onwards, the Annual Attestation Statement must attest that:

1. An ISMS consistent with the Core Requirements of this policy was in place during the financial year being reported on;
2. Taking into account the business requirements of the Department or Statutory Body, adequate security controls are in place to mitigate identified risks to digital information and digital information systems for the foreseeable future;
3. All Public Sector Agencies under the control of the Department or Statutory Body with a risk profile sufficient to warrant an independent ISMS have developed an ISMS in accordance with the Core Requirements of this policy;
4. Where applicable, certified compliance with *AS/NZS ISO/IEC 27001* by an accredited third party has been maintained during the financial year being reported on.

All Departments and Statutory Bodies must use the Annual Attestation Statement Template in this Annex.

A.1.1 TEMPLATE: Annual Attestation Statement

Digital Information Security Annual Attestation Statement for the 20XX-20XX Financial Year for [Department or Statutory Body]

I, [Department Head or Governing Board of the Statutory Body], am of the opinion that [Department or Statutory Body] had an Information Security Management System in place during the financial year being reported on consistent with the Core Requirements set out in the *Digital Information Security Policy for the NSW Public Sector*.

I, [Department Head or Governing Board of the Statutory Body], am of the opinion that the security controls in place to mitigate identified risks to the digital information and digital information systems of [Department or Statutory Body] are adequate for the foreseeable future.

I, [Department Head or Governing Board of the Statutory Body], am of the opinion that all Public Sector Agencies, or part thereof, under the control of [Department or Statutory Body] with a risk profile sufficient to warrant an independent Information Security Management System have developed an Information Security Management System in accordance with the Core Requirements of the *Digital Information Security Policy for the NSW Public Sector*.

I, [Department Head or Governing Board of the Statutory Body], am of the opinion that, where necessary in accordance with the *Digital Information Security Policy for the NSW Public Sector*, certified compliance with *AS/NZS ISO/IEC 27001 Information technology - Security techniques - Information security management systems - Requirements* had been maintained by all or part of [Department or Statutory Body] and all or part of any Public Sector Agencies under its control.

ANNEX B ANNUAL ATTESTATION & EVIDENCE OF CERTIFICATION

B.1 Annual Attestation and Evidence of Certification Requirements

Each NSW Government Shared Service Provider must:

1. Attest annually that an ISMS consistent with the Core Requirements of this policy was in place during the period being reported on;
2. Attest annually that adequate security controls are in place to mitigate identified risks to digital information and digital information systems for the foreseeable future; and
3. Provide evidence in writing annually of certification in accordance with Core Requirement 3.

The Executive Director or equivalent of each Shared Service Provider must use the Digital Information Security Annual Attestation & Evidence of Certification Statement Template in this Annex and include as an attachment written evidence of certification by an accredited third party.

The Digital Information Security Annual Attestation & Evidence of Certification Statement and written evidence should be sent to:

ICT Board
c/- ICT Policy
Department of Finance & Services
Level 17, McKell Building
2-24 Rawson Place
SYDNEY NSW 2000
E: informationsecurity@services.nsw.gov.au

B.1.1 TEMPLATE: Annual Attestation & Evidence of Certification Statement

Digital Information Security Annual Attestation & Evidence of Certification Statement for the 20XX-20XX Financial Year for [Shared Service Provider]

I, [name and title (Executive Director or equivalent)] of [Shared Service Provider], am of the opinion that [Shared Service Provider] had an Information Security Management System in place during the financial year being reported on consistent with the Core Requirements set out in the *Digital Information Security Policy for the NSW Public Sector*.

I, [name and title (Executive Director or equivalent)] of [Shared Service Provider], am of the opinion that the security controls in place to mitigate identified risks to the digital information and digital information systems of [name of Shared Service Provider] are adequate for the foreseeable future.

I, [name and title (Executive Director or equivalent)] of [Shared Service Provider], confirm that [name of Shared Service Provider] has maintained certified compliance with *AS/NZS ISO/IEC 27001 Information technology - Security techniques - Information security management systems - Requirements* by an accredited third party during the financial year being reported on. Evidence of certification is enclosed.

ANNEX C IMPLEMENTATION PROGRESS REPORT

C.1 Implementation Progress Report Requirements

Each NSW Government Department, Statutory Body and Shared Service Provider must respond to each of the actions in the Implementation Progress Report Template in this Annex on or before 31 July 2013 AND on or before 31 January 2014. Progress Reports must be sent to:

ICT Board
c/- ICT Policy
Department of Finance & Services
Level 17, McKell Building
2-24 Rawson Place
SYDNEY NSW 2000
E: informationsecurity@services.nsw.gov.au

C.1.1 TEMPLATE: Implementation Progress Report

Digital Information Security Policy Implementation Progress Report for [July 2013/January 2014] for [Department, Statutory Body or Shared Service Provider]

	Action	Response
1	An information security policy has been developed.	
2	A Senior Responsible Officer has been appointed.	
3	All digital information is classified to ensure it receives an appropriate level of protection.	
4	Access to digital information and digital information systems is monitored and controlled.	
5	Controls are in place to prevent unauthorised disclosure, modification, removal or destruction of digital information.	
6	Security is an integral part of information systems purchasing and maintenance.	
7	The security of digital information and digital information systems accessed, processed, communicated to, or managed by external parties is controlled.	
8	The security of digital information and software exchanged with external entities is maintained.	
9	Controls are place to counteract interruptions to business activities and to protect critical business processes from the effects of major failures of digital information systems or disasters.	
10	The timely resumption of business processes in the event of a major failure is ensured.	
11	Processes are in place for the communication of digital information security events and weaknesses associated with digital information systems.	

	Action	Response
12	Timely corrective action is taken to mitigate the effect of digital information security events.	
13	Digital information security events that pose a risk across the sector are communicated in a timely manner.	

ANNEX D DOCUMENT CONTROL

D.1 Document History

Status: Current

Version: 1.0

Approved by:

Approved on:

Issued by: Department of Premier and Cabinet

Contact: Dawn Routledge, Director Information, ICT Policy, Department of Finance & Services

Email: Dawn.Routledge@services.nsw.gov.au

Telephone: (02) 9372 7785

This Memorandum supersedes *M2007-04 Security of Electronic Information.*

D.2 Responsibilities

Implementation of the Policy and Procedures: ICT Policy, Department of Finance and Services

Updating and maintaining the Policy: ICT Policy, Department of Finance and Services