PART 1  PRELIMINARY

1.1  Scope

NSW Government has established its ICT Strategy to improve service delivery and derive better value from its investments. As part of the ICT Strategy, this policy establishes the security requirements for digital information in NSW Public Service Agencies.

The Digital Information Security Policy (DISP) covers a minimum set of controls, and requirements relating to certification, attestation and the establishment of the Digital Information Security Community of Practice.

1.2  Application

All NSW Public Service Agencies and Shared Service Providers must comply with Part 2 and Part 3 of this policy.

In accordance with Premier’s Memorandum M1999-19 Applyability of Memoranda and Circulars to State Owned Corporations, this policy does not apply to State Owned Corporations. This policy is however recommended for adoption in State Owned Corporations, as well as local councils and universities.

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 relevant legislation, regulations, Cabinet Conventions, policies and contractual obligations requiring information to be available, safeguarded or lawfully used.
- **Assurance** – to provide assurance to NSW Parliament and the people of NSW that information held by the Government is appropriately protected and handled.
PART 2 POLICY STATEMENT

Core Requirement 1—Information Security Management System

All NSW Public Service Agencies 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. ISO 31000 Risk management - Principles and guidelines
4. Agency business continuity and disaster recovery management

The Department Head must conduct a risk assessment to identify any business area or function to which risks apply. Agencies must review their ISMS annually or when any new risks are identified.

Core Requirement 2—Compliance with Minimum Controls

In developing the ISMS, all controls from ISO 27001 Information technology - Security techniques - Information security management systems – Requirements 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 ISO 27001.

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

<table>
<thead>
<tr>
<th>Security Category</th>
<th>ISO 27001:2013 and other Control(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Governance</td>
<td></td>
</tr>
<tr>
<td>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. The Information Security Management Systems (ISMS) must include the following governance arrangements:</td>
<td>A.5.1.1</td>
</tr>
<tr>
<td>o an Information Security Policy</td>
<td></td>
</tr>
<tr>
<td>o a designated individual (Senior Responsible Officer) responsible for digital security, and</td>
<td>A.6.1</td>
</tr>
<tr>
<td>o alignment to the agency’s internal audit and risk management policy, such as TPP09-05</td>
<td></td>
</tr>
</tbody>
</table>
### 2. Information security systems independent review

Agencies must independently review their ISMS annually or when there is a change to the level of risk to digital information and digital information systems.

- **A.18.2.1**

### 3. Information classification labelling and handling

All digital information must be assessed to determine its classification 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,
- Government Information (Public Access) Act 2009,
- State Records Act 1998,
- Health Records and Information Privacy Act 2002, and
- NSW Classification and Labelling Guidelines

- **A.8.2**
- **A.13.2**
- **A.18.1.3**
- **A.18.1.4**

### 4. Controlling access to information systems

Access to digital information and digital information systems must be monitored and controlled with regard to relevant laws and regulations, in particular those listed in category 3 (above).

- **A.9**
- **A.13.1**

### 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, with regard to relevant laws and regulations, in particular those listed in category 3 (above).

- **A.11**
- **A.12**
- **A.18.1.3**

### 6. Acquisition, development and maintenance of information systems and services

Security must be an integral consideration in the acquisition, development and maintenance of information systems and services.

- **A.14**
- **A.15**

### 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.

- **A.13.2**
- **A.15**

### 8. Business processes and continuity

Agencies must develop business continuity and disaster recovery plans to prepare for potential disasters and critical business function failures.

These plans must have controls to appropriately counteract interruptions to business activities and ensure that IT systems support the recovery of critical business processes.

- ISO 22301
- ISO 27031
- ISO 24762
Business continuity and disaster recovery plans must be tested at planned intervals.

9. Security incident management

Agencies must maintain appropriate contacts with relevant authorities. 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.

A.6.1.3
A.16.1

10. Collaboration and information sharing

A collaborative approach to information security, facilitated by the sharing of information security experience and knowledge, must be maintained.

A.6.1.4

11. Training and Awareness

Employees doing work that affects information security performance must understand the responsibilities of their role and take the initiative to remain aware of changes and maintain their skills through training and education, where necessary.

A.7.2.2

Core Requirement 3—Certified Compliance with ISO 27001

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

1. All Shared Service Providers; and
2. any Public Service Agency or part thereof, whose risk assessment, performed by their controlling agency, requires them to be certified.

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

In addition, certification may be shared across the sector where information security investment and standards have been achieved through common infrastructure and services.

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 Public Service Agencies and Shared Service Providers must maintain an up-to-date listing of their Senior Responsible Officer (SRO) with the Digital Information Security Community of Practice Register. The listing must include the SRO’s name, position, email address, and work and mobile telephone numbers.

Change of SRO, or a change of details, must be communicated within ten business days.
Core Requirement 5—Compliance Attestation

Departments and Statutory Bodies – Annual Attestation
Each Department and Statutory Body, as defined by the Public Finance and Audit Act 1983, 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 31 July each year.

Attestation and evidence of certification must be provided in accordance with ANNEX B of this policy.
PART 3  MAINTAINING COMPLIANCE

All Public Service Agencies and Shared Service Providers must comply with this policy and actions contained in this Part.

3.1 Maturity Progress Report

All SROs must report progress on the effectiveness of their ISMS on or before 28 February each year, and share their report with the Community of Practice.

3.2 Nomination to the Community of Practice

All Public Service Agencies and Shared Service Providers are to report the details and nomination (including replacements) of their SRO by email within 10 business days of the decision being made to the Digital Information Security Community of Practice Register at informationsecurity@finance.nsw.gov.au.

3.3 Information classification, labelling and handling

In October 2013, NSW Government published the *NSW Classification and Labelling Guidelines*. All Public Service Agencies and Shared Service Providers must comply with these Guidelines.
PART 4  NOTES AND GUIDANCE

4.1 Definitions

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

**Accredited Third Party:** a certification body or registrar that has been accredited by a body authorised by national government –in accordance with ISO 27006 *Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems*.

**Control:** a measure that modifies risk. Controls include any process, policy, device, practice, or other action that modifies risk. Controls may not always exert the intended or assumed modifying effect. [clause 2.16 ISO27000]

**Controlling agency:** For the purpose of this policy, this means ‘the capacity of an entity to dominate decision making, directly or indirectly, in relation to the financial and operating policies of another entity so as to enable that other entity to operate with it in pursuing the objectives of the controlling entity.’ *(Australian Accounting Standards 24 Consolidated Financial Reports).* Further details are also provided in *Australian Accounting Standards 29 Financial Reporting by Government Departments*.

**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.

**Head of a Public Service Agency:** in the case of a Department - the Secretary of the Department, or in any other case - the head of the related or separate agency.

**Function:** a power, authority or duty. *(Government Sector Employment Act 2013)*

**Information Security:** preservation of confidentiality, integrity and availability of information. In addition, other properties, such as authenticity, accountability, non-repudiation and reliability can also be involved. *(clause 2.33 ISO27000)*

**Information Security Event:** an identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of controls, or a previously unknown situation that may be security relevant. *(clause 2.35 ISO27000)*

**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. *(clause 2.36 ISO27000)*

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

**Outsourced service provider** means a third party organisation that provides corporate and other functions (such as those involving the recording, processing, storing and transferring of information on behalf of an agency) where the provision of those services has an impact on the agency’s system of internal control as it relates to digital information and digital information systems. An example would be ServiceFirst.
Public Service Agency: for the purposes of this policy, this includes:

- all agencies of the NSW public service as defined by the Government Sector Employment Act 2013 i.e. a Department, a Public Service executive agency (being an agency related to a Department), or a separate Public Service agency, and
- all Local Health Districts, Statutory Health Corporations and Statewide or Specialist Health Services.

Shared Service Provider: any entity that provides functions that are used by more than one Public Service Agency, whether they are internal or external.

Functions may include those relating to:

- operating or frontline services
- services within corporate functions, such as finance, human resources, and ICT

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

- Cabinet Conventions: NSW Practice (M2006-08)
- Government Sector Employment Act 2013
- Health Records and Information Privacy Act 2002
- Government Information (Public Access) Act 2009
- M1999-19 Applicability of Memoranda and Circulars to State Owned Corporations
- M2007-04 Security of Electronic Information
- NSW Government ICT Strategy
- NSW Information Classification and Labelling Guidelines
- NSW Public Service Commission Personnel Handbook
- 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
- State Records Act 1998

Standards

- Australian Accounting Standards 24 May 1992 Consolidated Financial Reports
- Australian Accounting Standards 29 June 1998 Financial Reporting by Government Departments
- ISO 27000 Information technology – Security techniques – Information security management systems – Overview and vocabulary
4.3 Supporting Documentation

- Australian Government Cyber Security Strategy
- Australian Signals Directorate: Strategies to Mitigate Targeted Cyber Intrusions
- Australian Signals Directorate: Top Four Mitigation Strategies to Protect Your ICT System
- Australian Government Attorney-General’s Department Protective Security Framework

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

An independent ISMS must be developed in accordance with this policy if the risks:

- would generally require management under an ISMS but are not managed by the parent Department; and
- are sufficiently specific to that business area or function that they can’t reasonably be included in an agency-wide ISMS.

Senior Responsible Officer

The Senior Responsible Officer (SRO) should:

- have sufficient influence to achieve the set ISMS objectives
- have relevant information security expertise, including with ISMS
- be able to participate in relevant information security activities, including receiving threat intelligence, responding to incidents and liaising with relevant authorities

The SRO should be a member of the NSW Public Service. It is also recommended that the SRO has a Senior Executive role and reports directly to the head of agency, Chief Information
Officer (CIO) or Chief Financial Officer. In smaller agencies, the SRO may also perform one of these roles. If the SRO is not also the CIO, it is recommended they are certified in one of the following, (or equivalent):

- Certified information security manager
- Certified Information System Auditor
- Certified Information Systems Security Professional
- Certified Risk and Information Systems Control
- 27001 Lead Auditor

The head of the Public Service Agency should determine if the role of the SRO is subject to the Criminal Records Check section (2-15) of the NSW Public Service Commission Personnel Handbook, based on the sensitivity of information it manages.

**Public Service Agencies that do not manage their own digital information or digital information systems**

It may be appropriate for agencies to outsource the storage and management of their digital information and digital information systems to outsourced service providers. In this case, the risks should be explicitly assessed in the ISMS risk assessment. Shared ownership and responsibility for managing the digital information and digital information systems should be clearly outlined in the ISMS and in any contractual or service level agreements with the service provider.

Where risk is managed by outsourced service providers, the ISMS should focus on Minimum Control 7, *Controlling relationships with suppliers and external parties*.

Agencies that manage risk with outsourced service providers must be satisfied that the outsourced service providers have sufficient controls in place to adequately protect the security of digital information and information systems of the Public Service Agency in accordance with this policy and statutory obligations.

Public Service Agencies that fall into this category are still required to satisfy Core Requirement 5—Compliance Attestation.

**Public Service Agencies with technologically autonomous sub-agencies**

The ISMS of a Department or Statutory Body may require a sub-agency, division or major business function to have an independent ISMS.

The development of an independent ISMS is an adequate control to mitigate the risk to the digital information and digital information systems of the sub-agency, division or business function.

The Department or Statutory Body does not need to 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 and maintained.

**Reviewing ISMS Maturity**

When planning and operating the ISMS, Public Service Agencies and Shared Service Providers are encouraged to self-assess the maturity of their security management using a maturity model it determines suitable.
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 ISO 27001 Information technology - Security techniques - Information security management systems - Requirements based on a thorough assessment of the risk to digital information assets and systems. Other ISO27000 series standards could also be considered such as ISO27014 for information security governance or ISO27031 for business continuity readiness.

Information security systems independent review
The requirement for independent review may be satisfied by certified compliance with ISO 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. Auditors should understand the digital information and digital information systems security environment but they should not have contributed directly to the development of the ISMS.

Independent review may be part of a peer review process or outsourced to external contractors who provide audit services, without the need for certification or accreditation.

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
Some examples of internal Shared Service Providers are:

- Government Data Centres - Office of Finance and Services
- Transport for NSW
- eHealth
- Business Services - Family and Community Services
- Fire and Rescue NSW

An example of an external Shared Service Provider is ServiceFirst.

When certification is required under Core Requirement 3
When performing risk assessments to determine whether certification is necessary, agencies should assess the impact on the controlling agency of loss of availability, integrity and confidentiality of information in the agency or sub-agency business functions.

Entities whose digital information systems contain particularly sensitive information, or whose systems are at a particularly high risk of a security event, are expected to identify themselves as requiring full compliance with the ISO 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 that is critical to the agency. The certification should cover the information assets that are most important and most at risk in terms of the likelihood and impact 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 SROs, information professionals and interested government personnel from all Public Service Agencies and Shared Service Providers. It will facilitate implementation of the policy, share best practice and disseminate information on risks that pose a threat to digital information and digital information systems across the NSW public sector.

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:

- 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/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
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.
4.5 Timetable of Key Dates

Table 3: Timetable of Key Dates

<table>
<thead>
<tr>
<th>Date</th>
<th>Deliverable</th>
<th>Affected Entities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Each Annual Reporting Period from 2015-16 onwards</td>
<td>Annual Attestation Statement to appear in Annual Report</td>
<td>All Departments and Statutory Bodies (as defined by the Public Finance and Audit Act 1983)</td>
</tr>
<tr>
<td>31 July each year from 2015 onwards</td>
<td>Annual Attestation and Evidence of Certification provided to the NSW Government ICT Board</td>
<td>All Shared Service Providers</td>
</tr>
<tr>
<td>28 February from 2016 onwards</td>
<td>Progress Report provided to Information Security Community of Practice</td>
<td>All Public Service Agencies and Shared Service Providers</td>
</tr>
</tbody>
</table>

4.6 Enquiries

General inquiries concerning this document should initially be directed to:

Director, Information
Service Innovation and Strategy
Office of Finance and Services
E: informationsecurity@finance.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 ISO 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, 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 participants from both public and private sector with experience in electronic information security, met to refine the key elements of the policy for approval by the ICT Board.

This Digital Information Security Policy was first published in November 2012 under Premier’s Memorandum M2012-15 Digital Information Security Policy. Agencies were required to implement the Policy by 31 December 2013.

This policy supersedes M2007-04 Security of Electronic Information.
ANNEX A     ANNUAL ATTESTATION

A.1 Annual Attestation Requirements

Each NSW Government Department and Statutory Body as defined by the Public Finance and Audit Act 1983 must include a Digital Information Security Annual Attestation Statement in its Annual Report under the section dealing with risk management and insurance activities.

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 controls are in place to mitigate identified risks to the digital information and digital information systems;

3. all sub-agencies, divisions and business functions under the control of the Department or Statutory Body have been assessed to determine if an independent ISMS is required in accordance with the Core Requirements of this policy; and

4. where applicable, certified compliance with ISO 27001 by an Accredited Third Party has been maintained during the year being reported on.

The following templates must be used for Annual Attestation Statements.

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, [name of Department Head or Governing Board of the Statutory Body], am of the opinion that [name of Department or Statutory Body] had an Information Security Management System in place during the 20xx-20xx financial year that is consistent with the Core Requirements set out in the NSW Government Digital Information Security Policy.

The controls in place to mitigate identified risks to the digital information and digital information systems of [name of Department or Statutory Body] are adequate.

A. There is no agency under the control of [name of Department or Statutory Body] which is required to develop an independent ISMS in accordance with the NSW Government Digital Information Security Policy.

B. Risks to the digital information and digital information system of [name of agencies, sub-agencies, divisions or business functions] have been assessed with an independent ISMS [developed/being developed/certified] in accordance with the NSW Government Digital Information Security Policy.

C. The [name of Department or Statutory Body] has maintained certified compliance with ISO 27001 Information technology - Security techniques - Information security management systems - Requirements by an Accredited Third Party during the 20xx-20xx financial year.

D. The [name of Department or Statutory Body] has maintained compliance with ISO 27001 Information technology - Security techniques - Information security management systems - Requirements and independently reviewed by [name of entity] during the 20xx-20xx financial year.
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 controls are in place to mitigate identified risks to the digital information and digital information systems; 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 should be sent to the ICT Board at informationsecurity@finance.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 of Executive Director or equivalent] of [Shared Service Provider], am of the opinion that [name of Shared Service Provider] had an Information Security Management System in place during the 20xx-20xx financial year that is consistent with the Core Requirements set out in the NSW Government Digital Information Security Policy.

The controls in place to mitigate identified risks to the digital information and digital information systems of [name of Shared Service Provider] are adequate.

[Name of Shared Service Provider] has maintained certified compliance with ISO 27001 Information technology - Security techniques - Information security management systems - Requirements by an Accredited Third Party during the 20xx-20xx financial year. Evidence of certification is enclosed.
C.1 Maturity Progress Report Requirements

Each SRO must respond to each of the actions in the Maturity Progress Report Template in this Annex on or before 28 February each year. Progress Reports must be sent to the Information Security Community of Practice at informationsecurity@finance.nsw.gov.au.

C.1.1 TEMPLATE: Maturity Progress Report

Digital Information Security Policy Maturity Progress Report for [name of Public Service Agency or Shared Service Provider]

<table>
<thead>
<tr>
<th>Action</th>
<th>Maturity level measured</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 ISMS governance is established and aligned to implementation of risk management policies.</td>
<td></td>
</tr>
<tr>
<td>2 ISMS is reviewed in accordance to the level of risks to digital information and digital information system.</td>
<td></td>
</tr>
<tr>
<td>3 All digital information is classified to ensure it is handled with appropriate level of protection under the NSW Government Information Classification and Labelling Guidelines.</td>
<td></td>
</tr>
<tr>
<td>4 Access to digital information and digital information systems is monitored and controlled.</td>
<td></td>
</tr>
<tr>
<td>5 Controls are in place and working effectively to prevent unauthorised disclosure, modification, removal or destruction of digital information.</td>
<td></td>
</tr>
<tr>
<td>6 Security requirements are considered and implemented as part of the acquisition, development and maintenance of information systems and services.</td>
<td></td>
</tr>
<tr>
<td>7 The security of digital information and digital information systems accessed, processed, communicated to, or managed by external parties is controlled.</td>
<td></td>
</tr>
<tr>
<td>8 The security of digital information and software exchanged with external entities is maintained.</td>
<td></td>
</tr>
<tr>
<td>9 Controls are in place to counteract interruptions to business activities and to ensure that IT systems support the recovery of critical business processes, and are tested at planned intervals.</td>
<td></td>
</tr>
<tr>
<td>10 The timely resumption of business processes in the event of a major failure is ensured.</td>
<td></td>
</tr>
<tr>
<td>11 Processes are in place for the communication of digital information security events and weaknesses associated with digital information systems within the agency and across the sector as appropriate.</td>
<td></td>
</tr>
<tr>
<td>12 Awareness training program is implemented and maintained.</td>
<td></td>
</tr>
</tbody>
</table>
ANNEX D      DOCUMENT CONTROL

D.1    Document History

Status: Approved
Version: 2.0
Approved by: ICT Board
Approved on: 1 April 2015
Issued by: Office of Finance and Services
Contact: Director Information, Service Innovation and Strategy, Office of Finance & Services
Email: informationsecurity@finance.nsw.gov.au Telephone: (02) 9372 8132

D.2    Responsibilities

Implementation of the Policy and Procedures:
Service Innovation and Strategy, Office of Finance and Services

Updating and maintaining the Policy:
Service Innovation and Strategy, Office of Finance and Services