Information Security Policy
# Table of Contents

**Document Control**
- Document information
- Document Control Log
- Document Approval
- Relevant Legislation & Associated Documents

**Foreword**

1. **Introduction**
   - 1.1 Scope
   - 1.2 Definitions
     - 1.2.1 Information Security
     - 1.2.2 Policy, Standards, Guidelines & Procedures

2. **Compliance with policy**
   - 2.1 Compliance
   - 2.2 Exemptions
   - 2.3 Compliance Audits

3. **Security policy**
   - 3.1 Information Security Infrastructure
   - 3.2 Review and evaluation

4. **Security Organisation**
   - 4.1 Organisation and Coordination
   - 4.2 Responsibilities
     - 4.2.1 Information Owners (Program Managers)
     - 4.2.2 Managers
     - 4.2.3 Information Custodians
     - 4.2.4 Information Users
     - 4.2.5 Corporate Information and Communications (CIC)
     - 4.2.6 IMT Steering Committee
     - 4.2.7 Management Committee
     - 4.2.8 Human Resources
     - 4.2.9 Internal Audit
     - 4.2.10 Third Party Access
     - 4.3 Outsourcing

5. **Asset classification and control**
   - 5.1 Asset Inventory
   - 5.2 Information Classification
     - 5.2.1 Classification Levels
     - 5.2.2 Default Label
     - 5.2.3 Labelling
     - 5.2.4 Need to know
     - 5.2.5 Private or Sensitive Information
   - 5.3 Electronic Records

6. **Personnel security**
   - 6.1 Prior to commencing work
   - 6.1.1 Responding to security incidents and malfunctions

7. **Physical and environmental security**
   - 7.1 Equipment security
   - 7.2 Security of equipment off-premises
<table>
<thead>
<tr>
<th>Section</th>
<th>Subject</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td><strong>Communications and operations management</strong></td>
<td>14</td>
</tr>
<tr>
<td>8.1</td>
<td>Malicious Software</td>
<td>15</td>
</tr>
<tr>
<td>8.2</td>
<td>Exchanges of information and software</td>
<td>15</td>
</tr>
<tr>
<td>9</td>
<td><strong>Access control</strong></td>
<td>15</td>
</tr>
<tr>
<td>10</td>
<td><strong>Systems development and maintenance</strong></td>
<td>15</td>
</tr>
<tr>
<td>10.1</td>
<td>Security Requirements of Systems</td>
<td>15</td>
</tr>
<tr>
<td>10.2</td>
<td>Security in Application Systems</td>
<td>15</td>
</tr>
<tr>
<td>10.3</td>
<td>Cryptographic controls</td>
<td>16</td>
</tr>
<tr>
<td>10.4</td>
<td>Security of system files</td>
<td>16</td>
</tr>
<tr>
<td>11</td>
<td><strong>Business continuity management</strong></td>
<td>16</td>
</tr>
<tr>
<td>12</td>
<td><strong>Compliance</strong></td>
<td>16</td>
</tr>
<tr>
<td>12.1</td>
<td>Software Compliance</td>
<td>16</td>
</tr>
<tr>
<td>12.2</td>
<td>Review of security policy and technical compliance</td>
<td>17</td>
</tr>
<tr>
<td>13</td>
<td><strong>Appendix A – Document Reference</strong></td>
<td>18</td>
</tr>
<tr>
<td>13.1</td>
<td>Relevant Legislation</td>
<td>18</td>
</tr>
<tr>
<td>13.2</td>
<td>Associated Documents</td>
<td>19</td>
</tr>
</tbody>
</table>
# Document Control

## Document information

<table>
<thead>
<tr>
<th>Document Category</th>
<th>Information Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Document Type</td>
<td>Policy</td>
</tr>
<tr>
<td>Document Number</td>
<td>CP04/3</td>
</tr>
<tr>
<td>Document Title</td>
<td>Information Security Policy</td>
</tr>
<tr>
<td>Subject</td>
<td>Policy covering how information Security is handled within State Records</td>
</tr>
<tr>
<td>Version</td>
<td>1.1</td>
</tr>
<tr>
<td>Author(s)</td>
<td>Mark Hofman</td>
</tr>
<tr>
<td>Release Date</td>
<td>24/9/2004</td>
</tr>
<tr>
<td>Maturity State</td>
<td>Final</td>
</tr>
<tr>
<td>Status</td>
<td>Released</td>
</tr>
<tr>
<td>Approved by</td>
<td>David Roberts, Director</td>
</tr>
<tr>
<td>Reviewed by</td>
<td>Michael Allen</td>
</tr>
<tr>
<td>Distribution List</td>
<td>All State Records staff and contractors (see 2.1 Compliance)</td>
</tr>
<tr>
<td>Storage</td>
<td><code>\Stamford\Workgroups\CIC\Government Relations\Compliance\Electronic Information Security\ISMS\Final\Information Security Policy.Doc</code></td>
</tr>
<tr>
<td>Restriction</td>
<td>UNCLASSIFIED</td>
</tr>
<tr>
<td>Last Review Date</td>
<td>23/9/2004</td>
</tr>
<tr>
<td>Review Time expires on</td>
<td>30/9/2005</td>
</tr>
</tbody>
</table>

1 These items are changed by editing the document properties. A link is provided on the tool bar. To view the changes use F9 to update the fields.

2 This item is updated automatically on saving the document. To view the changes use F9 to update the fields.
**Document Control Log**

All changes to this document must be recorded here.

Last Change made on 24/09/2004 9:06 by Michael Allen

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Authors</th>
<th>Summary of Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td>16/3/2004</td>
<td>Mark Hofman</td>
<td>Initial draft</td>
</tr>
<tr>
<td>1.0</td>
<td>8/7/2004</td>
<td>Mark Hofman, Michael Allen</td>
<td>Final corrections prior to submission</td>
</tr>
<tr>
<td>1.1</td>
<td>23/9/2004</td>
<td>Michael Allen</td>
<td>Minor amendments recommended by Executive</td>
</tr>
</tbody>
</table>

**Document Approval**

<table>
<thead>
<tr>
<th>Name (Position)</th>
<th>Signature</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>David Roberts (Director)</td>
<td></td>
<td>24/9/2004</td>
</tr>
</tbody>
</table>

**Relevant Legislation & Associated Documents**

This document and supporting policies support relevant legislation affecting State Records. A list of applicable legislation can be found in the Document Reference attached as Appendix A to this policy.

Likewise, this document and supporting policies refer to associated documents that provide more information on a topic, are procedures or are forms required. These are also listed in Appendix A.
State Records

Foreword

Information Security in State Records Authority

The New South Wales Government and the State Records Authority recognises that information systems are an important factor in governing the state and conduct the business of State Records as outlined in the State Records Act.

As a government organisation, State Records has obligations concerning information security, both to protect the government as well as the citizens of NSW. With this in mind, an Information Security Management System (ISMS) has been implemented within State Records providing a mechanism to address information security within the authority.

The ISMS is supported by this information security policy and supporting policies, addressing various aspects of information security.
1 Introduction

Information is an important asset to any organisation. Information Technology (IT) systems process much of the data that is used by State Records and play a key role in meeting organisational goals. Without accurate information, business functions cannot continue which has a detrimental impact on the organisation and potentially the NSW government.

This policy and supporting policies provide staff with instructions and guidance concerning Information Security allowing a consistent and appropriate approach to protecting the information assets of the organisation.

1.1 Scope

This policy applies to the State Records managed network and/or owned network components. This includes, but is not limited to:

- the Primary Firewall;
- all servers;
- all State Records issued equipment (laptops, workstations, etc.);
- routers connecting networks;
- remote sites;
- devices connecting to State Records owned equipment.

1.2 Definitions

Information Technology (IT) and IT Security use specific terms that may not be known to all. The concepts are described here.

1.2.1 Information Security

Information Security is the term used to describe the “the concepts, techniques, technical measures, and administrative measures used to protect information assets from deliberate or inadvertent unauthorized acquisition, damage, disclosure, manipulation, modification, loss, or use”\(^3\).

The goals of information security are to provide Confidentiality, Integrity and Availability (CIA). These three concepts are central to information security and must be kept in mind at all times when implementing technology.

- **Confidentiality** – the assurance that only authorised users have access and can manipulate the information;
- **Integrity** – the information provided is accurate and has not been tampered with;
- **Availability** – The required systems and the information, is available to those that require access when needed.

1.2.2 Policy, Standards, Guidelines & Procedures

There is often some confusion as to what the exact purpose of a specific type of document is. Within State Records, the following definitions will be used:

- **Policy** - An Information Security policy is a management instruction that outlines the role of Information Security within State Records, what the roles, and responsibilities of staff are, and provides guidance on security issues. The policy contains high level statements that are mandatory.

---

The Information security policy consists of this document and supporting issue specific documents.

- **Standards** - Standards contain the specific requirements that must be met. They provide information on how the organisation should implement/perform certain functions. State Records is working towards compliance with the AS/NZS 7799.2.2003 – Information security management standard.

  Internal to the organisation there may be additional standards that should be followed.

- **Guidelines** - Unlike policies, guidelines are optional. They are highly recommended and should be followed. For example the Password selection guidelines4 while not mandatory, are highly recommended to be used to select a strong password.

- **Procedures** - Procedures state how the standards, guidelines and policies are to be implemented. They are often detailed instructions on how to perform a certain task.

Policies are high level documents outlining what must be done, standards provide information on how the policy can be met, and guidelines support the standards and policies. Finally, procedures state how they can be implemented and provide detailed instructions.

# 2 Compliance with policy

## 2.1 Compliance

This information security policy applies to:

- all computer systems owned and/or managed by State Records, regardless of their location;
- all platforms (operating systems) deployed within the organisation;
- all computer sizes, ranging from Personal Digital Devices (PDA) through to corporate servers;
- all information handled by State Records systems;
- all applications and systems whether developed by State Records or purchased;
- all State Records staff that use State Records computing facilities, this includes but is not limited to full time employees, part-time or casual employees, contractors, subcontractors, consultants, etc;

All staff members are expected to be familiar with and comply with this policy. Violations of this policy can lead to revocation of system privileges and/or disciplinary action up to and including dismissal. Unlawful activities may be referred to the appropriate authorities for criminal/civil action.

## 2.2 Exemptions

It is recognised that under certain circumstances the requirements in this policy cannot be met. Exemptions to this policy are acceptable. However, they must be documented and approved in advance by the IMT Steering Committee.

In order to seek an exemption the request must be made in writing and submitted to CIC using the Exemption Request Form. The request will be evaluated and a recommendation made to the IMT Steering Committee.

---

4 Password Selection Guidelines provides information on how to select a strong password that meets the requirements of the policy.
2.3 Compliance Audits
The Information Security Policy, all additional supporting policies, standards, guidelines and procedures issued in support of the policy, form the basis on which security audits and adequacy assessments will be conducted.
These must be conducted at least once every eighteen months.

3 Security policy

3.1 Information Security Infrastructure
An information security policy provides the organisation with documentation that outlines how the organisation handles Information Security. The policy may be one or more documents, provided that clearly states the “rules” that must be followed in order to maintain an appropriate level of security within the organisation.

Relevant policies provide management direction and support for information security.
The following Information Security Policy infrastructure is in place within State Records

3.2 Review and evaluation
In order for the Information Security Policy to remain effective, it must be reviewed regularly, updated when changes are made and compliance with the policy evaluated on a regular basis.

Compliance with this policy must be evaluated at least once every twelve (12) months. This review can be performed by the Internal Audit function or other suitably qualified personnel not involved in the implementation or management of security within State Records.

This review must keep in mind:
- changes in technology;
- effectiveness of current policy and controls (this can be determined by the number and nature of any security incidents recorded);
• cost and impact of controls on the business.

4 Security Organisation

4.1 Organisation and Coordination

Information Security is a corporate issue. High level support for information security is provided by the IM&T Steering Committee, which consists of the executive and the CIO. This group will provide direction as well as support for Information Security initiatives within State Records.

Secondly, the Management Committee provides guidance and support at an operational level, this group consists of the executive and senior managers from each area.

Coordination of security within State Records, on behalf of the Steering Committee, will be performed by CIC.

Information Security skills are necessary to perform many security related tasks. While some security knowledge may be available within the organisation there will be occasions where specialist skills are required. If this is the case, external specialist resources will be engaged.

When a security event occurs, it may be necessary to contact law enforcement bodies, regulatory bodies, information services providers and telecommunications operators. State Records has good relationships with these organisations. They must be maintained, as they may be needed in the event of a security incident. Appropriate channels of communication with these organisations must be used.

New services that are to be provided to staff, the public, customers, or other third parties can have a significant impact. Changes to the environment must therefore be approved in order to provide appropriate control. Requests for new processing facilities must be submitted to and approved by the CIO. Depending on the size and impact, the Management Committee will need to authorise the request.

4.2 Responsibilities

Responsibilities for the protection of individual assets and for carrying out specific security processes must be clearly defined.

All staff within the organisation have some responsibilities concerning Information Security. These responsibilities are outlined here. Additional details regarding roles and responsibilities are provided in the appropriate issue specific policy.

4.2.1 Information Owners (Program Managers)

Information Owners play an important role in the organisation. They are ultimately responsible for the security of the systems they “own”.

Within State Records, all program managers are information owners. When information owners are not clearly implied by organisational design, the appropriate Associate Director will make the designation.

Information owners do not legally own the information in question; they are members of the management team who make decisions on behalf of the organisation in relation to the information. Information owners or their delegates are required to make the following decisions and perform the following activities:

(a) approve information-oriented access control privileges for specific job profiles;
(b) approve information-oriented access control requests which do not fall within the pure view of existing job profiles;
(c) select a data retention period for their information;
(d) designate a system-of-record (original source) for information from which all management reports will be derived;
(e) select special controls needed to protect information (such as additional input validation checks or more frequent back-up procedures);
(f) define acceptable limits on the quality of their information (accuracy, timeliness, time from capture to usage, etc.);
(g) approve all new and different uses of their information;
(h) approve all new or substantially enhanced application systems which use their information before these systems are moved into production operational status;
(i) review reports about system intrusions and other security events which are relevant to their information;
(j) review and correct reports which indicate the current production uses of their information;
(k) review and correct reports which indicate the job profiles which currently have access to their information;
(l) select a sensitivity classification category relevant to their information and review this classification every year, and;
(m) select a criticality category relevant to their information so that appropriate contingency planning can be performed.

Information owners must designate a back-up person to act if they are absent or unavailable. Owners may not delegate ownership responsibilities to third party organisations (such as outsourcing firms) or to any individual who is not a full-time employee of State Records. When both the owner and the back-up owner are unavailable, owner decisions may be made by the appropriate Associate Director.

4.2.2 Managers

Ordinary access control requests are not approved by owners. Instead, a staff member’s immediate manager approves a request for system access based on existing job profiles. If a job profile does not exist, it is the manager's responsibility to create the profile, obtain the approval of relevant Owners, and inform CIC. Similarly, when a worker leaves, it is the responsibility of their immediate manager to promptly inform the HR group who in turn will inform CIC so that the privileges associated with the staff member can be revoked.

4.2.3 Information Custodians

Custodians are in physical or logical possession of either State Records information or information that has been entrusted to State Records. Custodians operate systems on behalf of owners. While CIC staff members clearly are Custodians, local system administrators are also Custodians.

Whenever information is maintained only on a workstation, the User is also the Custodian. Each type of production application system information must have one or more designated Custodians.

Custodians are responsible for:

(a) safeguarding information under their control;
(b) implementing access control systems to prevent inappropriate disclosure;
(c) making back-ups so that critical information will not be lost;
(d) developing, documenting, and testing information systems contingency plans;
(e) implementing, operating, and maintaining the security measures defined by information Owners.
4.2.4 Information Users

Users are not specifically designated, but are broadly defined as any staff member with access to internal information or internal information systems. Users are required to:

(a) abide by all security requirements defined by Owners, implemented by Custodians, and/or established by CIC on behalf of the Management Committee;
(b) familiarise themselves with, and act in accordance with all State Records information security requirements as outlined in this document and the Acceptable Usage Policy;
(c) participate in information security training and awareness efforts where available;
(d) request access from their immediate manager, and;
(e) report all suspicious activity and security problems. These can be reported to CIC.

4.2.5 Corporate Information and Communications (CIC)

CIC is the central point of contact for all information security matters at State Records and coordinates security on behalf of the Management Committee. CIC provides internal technical expertise including security. It is this group’s responsibility to:

(a) balance security and operating requirements, taking into consideration the organisation, users, custodians and owners;
(b) define information security standards, procedures, policies, and other requirements applicable to the entire organisation;
(c) handle all access control administration;
(d) monitor security of State Records information systems;
(e) provide information security training and awareness programs to State Records staff;
(f) periodically providing management with reports about the current state of information security at State Records;
(g) respond, document and review virus infections, hacker break-ins, system outages, and similar security problems;
(h) assess the adequacy and co-ordinate the implementation of specific information security controls for new systems or services;
(i) Provides recommendations regarding exemptions to policy.

While information systems contingency planning is the responsibility of information Custodians, CIC must provide technical consulting assistance related to Business Continuity procedures and Disaster Recovery.

Where appropriate, CIC consults external expertise and acts as the facilitator.

4.2.6 IMT Steering Committee

The IMT Steering committee consists of the executive and the CIO. The purpose of the group is to decide on the direction of security within the organisation, it is the responsibility of this committee to:

(a) approve major initiatives to enhance information security;
(b) review and set policy relating to the acquisition and use of State Records’ computers, networks, associated equipment, and software, including security;
(c) review and approve overall responsibilities;
(d) ensure that security is part of the information planning process;
(e) agree specific methodologies and processes for information security, e.g. risk assessment, security classification system;
(f) approve exemptions to policy;
(g) agree specific roles and responsibilities for information security across the organisation.
4.2.7 Management Committee

The Management Committee consists of the executive and representatives of the operational and support programs. Concerning information security, their prime responsibility will be to provide direction and support for Information Security initiatives within State Records. In addition to this, it is the responsibility of the Management Committee to:

(a) monitor significant changes in the exposure of information assets to major threats;
(b) review and monitor information security incidents;
(c) support organisation-wide information security initiatives, e.g. security awareness program;
(d) promote the visibility of business support for information security throughout the organisation;
(e) determine required competencies for staff performing work effecting the ISMS
(f) provide competent training for staff performing ISMS duties;
(g) evaluate the effectiveness of training;
(h) maintain records of training, skill, experience and qualifications (skills register); and
(i) support general awareness training for all staff.

4.2.8 Human Resources

Information security is not only a technological issue, but also a human issue. The human Resources (HR) department plays an essential role in managing security.

HR has the responsibility to:

(a) verify information on applications, e.g. reference check;
(b) ensure that all staff have signed a confidentiality agreement before commencing work;
(c) notify CIC of new employees and terminations;
(d) ensure documentation such as the Confidentiality Agreement and terms and conditions are understood and have been signed by staff.

4.2.9 Internal Audit

Internal Audit at State Records is currently performed by the Internal Audit Bureau (IAB). The IAB will periodically perform compliance checks to make sure that the above-mentioned parties are performing their assigned duties, and to make sure that other information security requirements are being consistently observed.

Internal Audit acts as the eyes and ears of top management at State Records, making sure internal controls (including those related to information security) are consistent with both management expectations and organisational goals.
4.3 Third Party Access

There will be occasions when third parties require access to State Records resources in order to conduct business, perform maintenance tasks, or to deliver services.

In order to protect the environment all third party access must:

- be authorised by the appropriate system owner;
- in the case of new connections, have risks evaluated before connecting;
- connect in accordance with the Access Control Policy;
- be made aware of their responsibilities regarding security;
- be covered by a formal agreement which includes security requirements;
- be covered by a Confidentiality or Non Disclosure Agreement.

4.3.1 Outsourcing

Some functions are outsourced to external organisations. Outsourcing is defined as “a service performed on a regular basis under an agreed contract”. In some instances, the party delivering the services will need to have continuous or frequent access to State Records computing facilities, often to critical components. This access poses some risks that could lead to information being compromised. It is therefore essential that outsourcing requirements are managed and that security is included in such arrangements.

5 Asset classification and control

5.1 Asset Inventory

In order to protect assets they have to first be identified and valued. An inventory of important assets must be created and maintained. Owners must be clearly identified.

The assets to be documented should be:

- all information assets: databases and data files, system documentation, user manuals, training material, operational or support procedures, continuity plans, fallback arrangements, archived information;
- all software assets: application software, system software, development tools and utilities;
- all physical assets: computer equipment (processors, monitors, laptops, modems), communications equipment (routers, PABXs, fax machines, answering machines);
- all personal assets: information on the skill required to maintain and manage the systems in use within the organisation.
5.2 Information Classification

Information entrusted to State Records, must be protected in a manner commensurate with the value of the information, i.e. its sensitivity, criticality. While all data must be protected consistently, there may be additional requirements and restrictions depending on the label. This will be indicated by the classification or sensitivity label accompanying the data.

State Records will be following the its "Labelling of Sensitive Information" procedure developed in conjunction with the OIT guideline\(^5\). For further details regarding the preparation, handling, storage, copying, and disposal and so on, please refer to the internal and OIT guidelines.

5.2.1 Classification Levels

The levels in use within State Records are\(^6\):

- **PUBLIC** - This information has been specifically approved for public release or is available to the public. Unauthorised disclosure of this information will not cause problems for State Records, its customers, or its business partners. For example, brochures and material posted to State Records’ public Web pages. Disclosure of State Records information to the public requires the existence of this label, the specific permission of the information owner, or long-standing practice of publicly distributing the information.

- **UNCLASSIFIED & X-IN-CONFIDENCE** – UNCLASSIFIED is available to State Records staff only, X can be any of the following, 'BOARD', 'COMMERCIAL', 'EXECUTIVE', 'MANAGERS', 'DIRECTOR' and 'STAFF' and are available to certain staff members within the organisation. For detailed descriptions of these levels and the caveats that apply, please see the “Labelling of Sensitive Information” guidelines.

Information labelled as UNCLASSIFIED or X-IN-CONFIDENCE, is information whose compromise could cause limited damage to NSW, the Government, commercial entities, or members of the public, for example:

- cause substantial distress to individuals or private entities;
- cause financial loss or loss of earning potential to, or facilitate improper gain or advantage for individuals or private entities;
- prejudice an investigation;
- facilitate the commission of crime;
- breach proper undertakings to maintain the confidence of information provided by third parties;
- impede the effective development or operation of government policies;
- breach statutory restrictions on disclosure of information;
- disadvantage the Government in commercial or policy negotiations with others;
- undermine the proper management of the public sector and its operations.

Within State Records, the UNCLASSIFIED and X-IN-CONFIDENCE labels correspond to the caveats applied to the data within TRIM.

- **PROTECTED** - Information whose compromise could cause damage to NSW, the Government, commercial entities or members of the public, for example:

---


\(^6\) Descriptions for X-IN-CONFIDENCE, PROTECTED and HIGHLY PROTECTED have been extracted from the OIT Guideline "Guide to Labelling Sensitive Information".
Information Security Policy

- endanger individuals and private entities;
- work substantially against state or national finances or economic or commercial interests;
- substantially undermine the financial viability of major organisations;
- facilitate the commission of serious crime;
- seriously impede the development or operation of major government policies.

- HIGHLY PROTECTED - Information whose compromise could cause serious damage to NSW, the Government, commercial entities or members of the public, for example:
  - threaten life directly;
  - seriously prejudice public order;
  - substantially damage state or national finances or economic and commercial interests.

Information must be classified by the information owner. It is expected that the PROTECTED and HIGHLY PROTECTED categories will be used infrequently.

5.2.2 Default Label

All information not labelled otherwise is designated as UNCLASSIFIED.

5.2.3 Labelling

It is up to the owner or creator of information to designate an appropriate label, and up to the user or recipient of this information to consistently maintain an assigned label. Labels for sensitive information should be used in the subject field of electronic mail messages or paper memos. Labels for sensitive information should appear on:

- Floppy diskettes;
- magnetic tape reels;
- CD-ROMs;
- Printed documents;
- Audiocassettes;
- and other storage media.

If a storage volume (such as a floppy diskette) contains information with multiple classifications, the most sensitive category should appear on the outside or overall label. Likewise, when creating a collection of information from sources with various classifications, the collection must be classified at the highest sensitivity level of the source information.

For further information, see the “Procedure for Labelling Sensitive Information”.

5.2.4 Need to know

All access is on a need to know basis. This means that even though a document or file may be labelled as UNCLASSIFIED and thus is restricted to State Records staff only, this does not imply that all State Records staff may access the document. There must be a “need to know”.

UNCLASSIFIED
5.2.5 Private or Sensitive Information

State Records is subject to the Privacy and Personal Information Protection Act 1998 and has developed an internal Privacy Management Plan to clarify to staff their obligations under these principles.

State Records uses the definitions of personal data as outlined in the act. Sensitive data are a subset of personal information and are covered in the act through restrictions:

- **Personal information** - Information or an opinion (including information or an opinion forming part of a database) whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion. It includes all personal information regardless of its source.

- **Sensitive information** - is a subset of personal information such as health data, religious beliefs, political opinions, etc.

Information classified X-IN-CONFIDENCE or higher, can additionally be labelled PRIVATE, or SENSITIVE.

Information classified as UNCLASSIFIED cannot contain PRIVATE or SENSITIVE information under any circumstances.

For further information, consult the State Records Privacy Management Plan on the intranet.

5.3 Electronic Records

State Records administers the State Records Act and must comply with the Act itself.

The NSW government in Memorandum No 98-16 Records Management Standards and Policies outlines the requirements for all agencies adopting the Electronic Recordkeeping and Electronic Messages as Records policies as published by State Records Authority of NSW (State Records).

In line with these policies, State Records views all “recorded information, in any form, including data in computer systems, created or received and maintained by an organisation or person in the transaction of business or the conduct of affairs and kept as evidence of such activity” as records.

All records within State Records must be managed as outlined in the Policy on Electronic Messages as Records, the Policy on Electronic Recordkeeping, and the State Records “Records Management Procedures” for the central records function.

All Electronic records in State Records are managed within TRIM. Classifications are applied

---

7 Within TRIM, the product used to manage records, it is possible to restrict access to documents within a file. It is acceptable for UNCLASSIFIED files within TRIM to contain PRIVATE or SENSITIVE information, providing access lists are used to control access.

6 Personnel security

Information security is the responsibility of all staff members of State Records. In order to provide staff with clear direction concerning their responsibilities, where appropriate the responsibilities must be documented in the job descriptions and the terms and conditions of employment.

All staff members and where relevant, third party users shall receive appropriate training and regular updates of State Records policies and procedures.

6.1 Prior to commencing work

Prior to commencing work,

- **Reasonable verification of the claims made in the application must be completed** – references, credentials and other relevant information provided as part of the application must be verified.

- **The new staff member must receive relevant information and training regarding Information Security** – By providing training and documentation the importance of security is highlighted and the employee know what is expected of them.

- **Confidentiality agreements must be signed** - During the course of employment, staff may be exposed to information that is confidential. In order to help protect this information it is essential that a confidentiality Agreement is in place preventing the person from disclosing information to a third party while they are in the employ of State Records as well as when employment is terminated.

- **Applicable policies provided, read, understood, and signed** – Policies can only be enforced if they are published, read, and understood. By signing an acceptance document, the staff member indicates that they have read and understood the policies and will abide by its rules.

6.1.1 Responding to security incidents and malfunctions

Security incidents, weaknesses and software malfunctions must be reported to CIC and recorded in the helpdesk system as soon as possible after the incident is discovered. By recording these incidents management can be provided with accurate security and fault details. This allows State Records to correct the issue and minimise the impact the incident or malfunction may have on the organisation.

7 Physical and environmental security

In order to protect computing resources from accidental or deliberate damage physical access to those machines will be restricted to those that require access. Further details can be found in the Network Management Policy.

All State Records premises must be accessible only to authorised personnel, areas that store PROTECTED or HIGHLY PROTECTED data must be secured and allow access only to those that have a need to know.
7.1 Equipment security
Production servers must be housed in the machine rooms or other secure locations, which provide environmental controls such as air-conditioning, power management, and access control.

Equipment must be maintained in accordance with manufacturer requirements.

Activities affecting the physical infrastructure of the State Records network must be authorised by CIC. This includes, but is not limited to activities such as:

- cabling;
- scheduled power interruptions;
- telecommunications cabling;
- equipment maintenance.

7.2 Security of equipment off-premises
Equipment may be taken off site for a number of reasons. A laptop assigned to a staff member, equipment sent for repair to a vendor, etc. Equipment to be taken off-site, i.e. removed from State Records controlled premises, must only be taken when authorised to do so. Before removing equipment off premises a log entry must be made to record removal of the item.

Reasonable steps must be taken to ensure the safety and security of the equipment and the data contained on it whilst it is off-premises.

Computing equipment off-premises must not contain data labelled PROTECTED or HIGHLY PROTECTED.

Information must be erased from equipment prior to disposal or re-use.

8 Communications and operations management
In order to ensure the correct and secure operation of information processing facilities:

- controls will be in place to protect the network from unauthorised access;
- changes to processing facilities must be controlled and implemented according to the change management procedures;
- procedures identified in this policy and supporting policy must be documented and maintained, including incident management procedures;
- development and production environments must be separate;
- duties, where required and feasible should be segregated;
- external facilities must be used with care and only after the risks have been identified and appropriate controls agreed; capacity on critical systems must be monitored;
- all data and systems on production servers must be backed up regularly and off-premises copies kept;
- operational staff must maintain a log of their activities;
- faults shall be reported and corrective action taken;
- information labelled X-IN-CONFIDENCE (see 5.2.1 Classification Levels above) or higher must not be removed from State Records premises without authorisation;
- all media must be handled in accordance with the Network Management Policy.

Further information on each of the above is available in the Network Management Policy.
8.1 Malicious Software
Malicious code or software such as viruses, Trojans, logic bombs, and blended threats can cause a lot of damage, both in lost time as well as through destruction of important information. In order to prevent this State Records utilises recognised anti-virus products to scan and clean all transmissions into and out of the organisation. Staff must take care when accessing the Internet and using floppy disks or other removable media to transfer information to State Records’ workstations.

8.2 Exchanges of information and software
Information and software is exchanged between State Records and other organisations. This may be through access to services provided by State Records or otherwise. Any information exchange, occurring on a regular basis must be bound by an agreement. The information exchanged must be protected in accordance with this policy.

Information designated as UNCLASSIFIED must be authorised for release by the director or his appointed delegate, before being published in any form.

Electronic commerce shall be protected against fraudulent activity, contract dispute and disclosure or modification of information.

9 Access control
Access to State Records computing resources will be in accordance with the Access Control Policy.

State Records adopts the security philosophy that all access is denied unless explicitly given.

Access to PUBLIC and UNCLASSIFIED information is not necessarily restricted with access controls that discriminate by user. On the other hand, access to information classified otherwise will be given only when a business need has been demonstrated and access has been approved by the system owner.

Likewise, access to special hardware and/or software (such as diagnostic test equipment called "sniffers") must be restricted based on business need.

10 Systems development and maintenance
State Records has an externally developed application on which some additional development as well as maintenance takes place.

Items that typically must be addressed are:

- input data validation;
- validation checks of internal processes;
- message authentication where required;
- output data validation.

For continued maintenance, any system developed must be adequately documented.

10.1 Security Requirements of Systems
When developing new systems or providing enhancements to existing applications security must be incorporated into the design and be part of the development life cycle.

10.2 Security in Application Systems
In order to prevent loss, modification and misuse of an application the data input and outputs must be validated. Where relevant, message authentication must be used as well as routines that aid detection of corrupted data.
10.3 Cryptographic controls
State Records currently does not have any requirements for Cryptography within the organisation. Should encryption or other data protection be required, CIC must be contacted as they can provide, or source, appropriate advice and facilities.

For cryptographic requirements for network connections, please see the Network Management Policy.

10.4 Security of system files
System files are the core of the servers that provide services to State Records, its customers and the public. In order to protect them and to maintain the integrity of the system changes must be made in accordance with the Change Control Procedures, i.e. each change must be approved, authorised and tested before implementation.

Where possible, production data must not be used in testing of systems or applications. If this is not possible, then the same access restrictions and controls applied to production data must be applied to the test data.

Source code, like system files must be protected to maintain the integrity and confidentiality of the data.

11 Business continuity management
Risk management is a focus for State Records. In light of this, Business Continuity (BC) is an essential component of State Records business. In order to counteract interruptions to business activities and to protect critical business processes from the effects of major failures or disasters. State Records will have documented BC processes and procedures.

A single framework of business continuity plans shall be maintained to ensure that all plans are consistent, and to identify priorities for testing and maintenance. Business continuity plans shall be tested regularly and maintained by regular reviews to ensure that they are up to date and effective.

12 Compliance
Compliance with this and supporting policies will allow State Records to avoid breaches of any criminal and civil law, and statutory, regulatory, or contractual obligations. The applicable legislations apply to State Records as a whole and no system is exempt.

12.1 Software Compliance
State Records provides a sufficient number of licensed copies of authorised software such that staff can perform their duties in an expedient and effective manner.

Should there be a requirement for additional licences, new software or changes to existing licences, CIC will make the appropriate recommendation or arrangements.

**State Records reserves the right to remove any software that has not been authorised or is not appropriately licensed.**
12.1.1.1 Unauthorised Copying
Staff must not make copies of or use software unless they know that the copies are in keeping with the vendor’s license to State Records. If a system which is used to process State Records information has been set-up by CIC, staff can rely on the fact that all software on this system is licensed and authorised.
Questions about licensing should be directed to CIC, which maintains documentation reflecting software licenses throughout State Records.
Making regular back-ups of software for contingency planning purposes is permissible.

12.2 Review of security policy and technical compliance
Managers have the responsibility to ensure that all security procedures within their area of responsibility are carried out correctly. This policy and technical compliance to the policy must be reviewed regularly.
Audits must be planned and agreed to minimise the risk of disruption to business. Tools used in this process must be authorised for use by CIC. They must not be used by any other than those conducting the audit.
13 Appendix A – Document Reference

13.1 Relevant Legislation

Policies support the organisation in meeting its business goals. In addition, they help the organisation to meet their legal obligations. This document outlines those laws and regulations that affect the organisation and have to be met.

The following table shows the relevant legislation that applies. Complete references of the acts can be found online at the Australasian Legal Information Institute http://www.austlii.edu.au.

- Anti-Discrimination Act, 1977
- Cyber Crimes Act, 2000
- Disability Discrimination Act, 1992
- Equal employment Opportunity (Commonwealth Authorities) Act, 1992
- Freedom of Information Act 1989
- Independent Commission against Corruption Act, 1988
- Industrial Relations Act, 1996
- Occupational Health and Safety Act, 2000
- Privacy Act 1988
- Privacy and Personal Information Protection Act (NSW) 1998
- Public Finance and Audit Act, 1983
- Public Sector Employment and Management Act, 2002
- Racial Discrimination Act, 1975
- Sex Discrimination Act, 1984
- State Records Act, 1998
- Telecommunications (Interception) Act, 1979
- Telecommunications Act, 1997
- The Crimes Act, 1900 (NSW)
- The Crimes Act, 1914 (Federal)
13.2 Associated Documents

There are a number of documents that support the policies and guidelines developed. A reference to those documents can be found here:

<table>
<thead>
<tr>
<th>Associated document</th>
<th>location</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Framework</strong></td>
<td></td>
</tr>
<tr>
<td>Information Security Management System Framework</td>
<td></td>
</tr>
<tr>
<td><strong>Policies</strong></td>
<td></td>
</tr>
<tr>
<td>Information Security Policy</td>
<td></td>
</tr>
<tr>
<td>Acceptable Usage Policy</td>
<td></td>
</tr>
<tr>
<td>Network Management Policy</td>
<td></td>
</tr>
<tr>
<td>Access Control Policy</td>
<td></td>
</tr>
<tr>
<td><strong>Standards</strong></td>
<td></td>
</tr>
<tr>
<td>AS/NZS 7799.2.2003</td>
<td>Standards Australia</td>
</tr>
<tr>
<td><strong>Guidelines</strong></td>
<td></td>
</tr>
<tr>
<td>Password Selection Guidelines</td>
<td></td>
</tr>
<tr>
<td>Guide to Labelling Sensitive Information</td>
<td></td>
</tr>
<tr>
<td><strong>Procedures</strong></td>
<td></td>
</tr>
<tr>
<td>Incident Management</td>
<td></td>
</tr>
<tr>
<td>Reporting Security Incidents</td>
<td></td>
</tr>
<tr>
<td><strong>Forms</strong></td>
<td></td>
</tr>
<tr>
<td>Exemption Request Form</td>
<td></td>
</tr>
<tr>
<td>Risk Acceptance Form</td>
<td></td>
</tr>
<tr>
<td>Security Incidents or Issues Reporting Form</td>
<td></td>
</tr>
<tr>
<td>------------------------------------------</td>
<td>---</td>
</tr>
<tr>
<td>Incident Form</td>
<td>Attached as Appendix A to Incident Management Process</td>
</tr>
</tbody>
</table>