



Security Policy

Confidentiality: Public
Prepared By:
Version:
Date: 12 May 2004

Approver's Name: Mike Grillo
Title: Chief Technology Officer

Signature:

Date Approved:

Document Control

Document Location

Q:\General Share Drive\Web updates\post to new site\Security\revised\CTO_P4.1_Security_Policy.doc

Electronic Records Management Information

File Folder Number: OCIO08/0xxx – Document Number: 08OCIOxxxxx

Author(s)

Function / Role

Author

Role

Revision by

Version

Date

Initial draft and consultation

Distributed to

Version

Date

Confidentiality Classification Table

	Confidentiality	Description	Circulation Limit (on a "NEED TO KNOW" basis)
<input type="checkbox"/>	Highly Protected	Unauthorised release could reasonably be expected to cause serious harm to an organisation or individual, or give unfair advantage to any entity or violate somebody's right to privacy.	Secure and highly restricted access.
<input type="checkbox"/>	Protected	Unauthorised release could reasonably be expected to cause harm to an organisation or individual, or give unfair advantage to any entity or violate somebody's right to privacy.	Confidential and limited access within ICT Sourcing and to authorised SA Government employees only.
<input type="checkbox"/>	Commercial-in-Confidence	Unauthorised release might possibly cause harm to an organisation or individual, or give unfair advantage to any entity or violate somebody's right to privacy.	Restricted use internally within SA Government and to authorised industry partners only.
<input type="checkbox"/>	Unclassified	No special classification is assigned.	No special restrictions other than legislative or administrative requirements.
<input checked="" type="checkbox"/>	Public	No harm could be caused to an organisation or individual, and no unfair advantage could be given to any entity and no violation would occur to somebody's right to privacy.	Unrestricted access.

Need-to-know - A person must have a legitimate need to access the security classified resources to carry out their official duties. Other justifications, such as position of authority, or the desire to enter controlled areas or access information for the sake of convenience, are not valid.

Table of Contents

TABLE OF CONTENTS	3
1. BACKGROUND	5
1.1 Context	5
1.2 Policy and Standards Statements	5
1.3 Rationale & Background	5
2. IMPLEMENTATION.....	6
2.1 Implementation Considerations	6
2.2 Responsibilities	6
Information Security Risk Management Chapter 2	7
Security Policy Chapter 3	7
Security Organisation Chapter 4.....	7
Asset Classification and Control Chapter 5.....	7
Personnel Security Chapter 6	7
Physical and Environmental Security Chapter 7.....	8
Communications and Operations Management Chapter 8	8
Access Control Chapter 9.....	9
Systems Development and Maintenance Chapter 10	10
Business Continuity Planning Chapter 11	10
Compliance Chapter 12.....	11

CTO/P4.1 SECURITY INFORMATION SECURITY MANAGEMENT FRAMEWORK

CTO/P4.1 Security – Information Security Management Framework

Security Classification:	Public	Version:	2.3.1	Status:	Approved
Audience:	SA Government Agencies	Compliance:	Mandatory		
Mandate/Authority:	Cabinet	Creator:	Government ICT Services		
Authorisation Date:	28 April 2003	Primary Contact:	Strategy & Operations		
Last updated:			Government ICT Services Division		
Expiry Date:	30 June 2007		Department for Transport, Energy and Infrastructure		
Publication Date:	10 May 2007		Tel: 8226 3558		

Coverage:

The South Australian public authorities required to adhere to this Standard are defined in CTO/P1.1 Government Policy on Information & Communication Technology – Governance – Compliant Authorities.

This policy or standard is intended for use by South Australian Government agencies only. Reliance upon this policy or standard by any other person is entirely at their own risk and the Crown in the right of South Australia disclaims all responsibility or liability to the extent permissible by law for any such reliance.

Managed and Maintained by
[Government Information and Communication
Technology Services / DTEI](#)

[Copyright](#) © Department for Transport, Energy and
Infrastructure 2003, 2004, 2007
[Disclaimer](#)
This page was last modified 12 May 2004

1. BACKGROUND

1.1 Context

The Information Security Management Framework presents a set of policies, standards, guidelines and control mechanisms for South Australian Government Agencies to use in developing their Information security capabilities. It has been designed as a practical, useable framework that can be readily implemented by South Australian Government Agencies. It addresses all aspects of security that are relevant to an Agency's use of Information and Communication Technology Services (ICT) to support and advance its business objectives. This includes issues such as physical and logical access control, data integrity and confidentiality, and the availability of ICT services. ICT environments of all types and complexities, from single workstations to large mainframes and highly distributed or networked systems are accommodated.

The framework has been written and structured to align closely with AS/NZS ISO/IEC 17799:2001 Information Technology – Code of Practice for information security management and AS/NZS 7799.2:2000 – Specification for information security management systems.

1.2 Policy and Standards Statements

Policy statements together with associated standards are included in the Information Security Management Framework document and can be accessed at:

<http://www.cto.sa.gov.au/architecture-and-standards/policies-and-standards/security/information-security-management-framework>

An index is included as Table 1 below.

1.3 Rationale & Background

Information and the supporting processes, systems and networks are important business assets. Confidentiality, integrity and availability of information may be essential to maintain competitive edge, cash flow, profitability, legal compliance and commercial image.

Increasingly, Agencies and their information systems and networks are faced with security threats from a wide range of sources, including computer-assisted fraud, espionage, sabotage, vandalism, fire and flood. Sources of damage such as computer viruses, computer hacking and denial-of-service attacks have become more common, more ambitious and increasingly sophisticated.

Dependence on information systems and services means Agencies are more vulnerable to security threats. The interconnecting of public and private networks, and sharing of information resources increases the difficulty of achieving access control. The trend to distributed computing has weakened the effectiveness of central, specialist control.

Many information systems have not been designed to be secure. The security that can be achieved through technical means is limited, and should be supported by appropriate management and procedures. Identifying which controls should be in place requires careful planning and attention to detail. Information security management needs, as a minimum, participation from suppliers, customers or shareholders. Specialist advice from outside organisations may also be needed.

Information security controls are considerably cheaper and more effective if incorporated at the requirements specification and design stage.

2. IMPLEMENTATION

2.1 Implementation Considerations

Exemptions: Advice regarding exemptions from this policy is provided in the Government Policy on Information and Communications Technology entitled 'Governance – Exemptions. An exemption provision that is specific to a particular policy, standard or procedure will be included in the relevant document.

2.2 Responsibilities

Security is a management issue. Chief Executives have ultimate responsibility for all security matters within their agencies.

Treasurer's Instruction 2, "Financial Management Policies" and the Financial Management Framework, Section 2, establish certain obligations and expectations on how entities of the South Australian Government manage their ICT systems. On the issue of Information Security Management, it is clearly required that the entity implements whatever control measures are necessary to provide adequate protection for its information.

TABLE 1**Security Policies and Standards**

		Chapter
Information Security Risk Management		2
Policy	Risk Management	2.1
Standard	Risk Identification and Assessment	2.1.1
 Security Policy		 3
Policy	Information Security Policy	3.1
Standard	Information Security Policy Document	3.1.1
Standard	Review and Evaluation	3.1.2
 Security Organisation		 4
Policy	Information Security Infrastructure	4.1
Standard	Management Information Security Forum	4.1.1
Standard	Information Security Co-Ordination	4.1.2
Standard	Allocation of Information Security Responsibilities	4.1.3
Standard	Authorisation Process for Information Processing Facilities	4.1.4
Standard	Specialist Information Security Advice	4.1.5
Standard	Co-Operation Between Organisations	4.1.6
Standard	Independent Review Of Information Security	4.1.7
Policy	Security Of Third Party Access	4.2
Standard	Identification of Risks from Third Party Access	4.2.1
Standard	Security requirements in third party contracts	4.2.2
Policy	Outsourcing	4.3
Standard	Security Requirements In Outsourcing Contracts	4.3.1
 Asset Classification and Control		 5
Policy	Accountability for Assets	5.1
Standard	Inventory of Assets	5.1.1
Policy	Information Classification	5.2
Standard	Classification Guidelines	5.2.1
Standard	Information Labelling and Handling	5.2.2
 Personnel Security		 6
Policy	Security In Job Definition and Resourcing	6.1
Standard	Including Security in Job Responsibilities	6.1.1
Standard	Personnel Screening and Policy	6.1.2
Standard	Confidentiality Agreements	6.1.3
Standard	Terms and Conditions of Employment	6.1.4

Policy	User Training	6.2
Standard	Information Security Education and Training	6.2.1
Policy	Responding to Security Incidents and Malfunctions	6.3
Standard	Reporting Security Incidents	6.3.1
Standard	Reporting Security Weaknesses	6.3.2
Standard	Reporting Software Malfunctions	6.3.3
Standard	Learning from Incidents	6.3.4
Standard	Disciplinary Process	6.3.5
Physical and Environmental Security		7
Policy	Secure Areas	7.1
Standard	Physical Security Perimeter	7.1.1
Standard	Physical Entry Controls	7.1.2
Standard	"Securing Offices, Rooms and Facilities"	7.1.3
Standard	Working in Secure Areas	7.1.4
Standard	Isolated Delivery and Loading Areas	7.1.5
Policy	Equipment Security	7.2
Standard	Equipment Siting and Protection	7.2.1
Standard	Power Supplies	7.2.2
Standard	Cabling Security	7.2.3
Standard	Equipment Maintenance	7.2.4
Standard	Security of Equipment Off-Premises	7.2.5
Standard	Secure Disposal or Re-Use of Equipment	7.2.6
Policy	General Controls	7.3
Standard	Clear Desk and Clear Screen Policy	7.3.1
Standard	Removal of Property	7.3.2
Communications and Operations Management		8
Policy	Operational Procedures and Responsibilities	8.1
Standard	Documented Operating Procedures	8.1.1
Standard	Operational Change Control	8.1.2
Standard	Incident Management Procedures	8.1.3
Standard	Segregation of Duties	8.1.4
Standard	Separation of Development and Operational Facilities	8.1.5
Standard	External Facilities Management	8.1.6
Policy	System Planning and Acceptance	8.2
Standard	Capacity Planning	8.2.1
Standard	System Acceptance	8.2.2
Policy	Protection Against Malicious Software	8.3
Standard	Controls Against Malicious Software	8.3.1
Policy	Housekeeping	8.4
Standard	Information Back-Up	8.4.1
Standard	Operator Logs	8.4.2
Standard	Fault Logging	8.4.3

Policy	Network Management	8.5
Standard	Network Controls	8.5.1
Policy	Media Handling and Security	8.6
Standard	Management of Removable Computer Media	8.6.1
Standard	Disposal Of Media	8.6.2
Standard	Information Handling Procedures	8.6.3
Standard	Security Of System Documentation	8.6.4
Policy	Exchange of Information and Software	8.7
Standard	Information And Software Exchange Agreements	8.7.1
Standard	Security of Media in Transit	8.7.2
Standard	Electronic Commerce Security	8.7.3
Standard	Security of Electronic Mail	8.7.4
Standard	Security of Electronic Office Systems	8.7.5
Standard	Publicly Available Systems	8.7.6
Standard	Other Forms Of Information Exchange	8.7.7
Access Control		9
Policy	Business Requirement for Access Control	9.1
Standard	Access Control Policy	9.1.1
Policy	User Access Management	9.2
Standard	User Registration	9.2.1
Standard	Privilege Management	9.2.2
Standard	User Password Management	9.2.3
Standard	Review Of User Access Rights	9.2.4
Policy	User Responsibilities	9.3
Standard	Password Use	9.3.1
Standard	Unattended User Equipment	9.3.2
Policy	Network Access Control	9.4
Standard	Policy on Use of Network Services	9.4.1
Standard	Enforced Path	9.4.2
Standard	User Authentication for External Connections	9.4.3
Standard	Node Authentication	9.4.4
Standard	Remote Diagnostic Port Protection	9.4.5
Standard	Segregation In Networks	9.4.6
Standard	Network Connection Control	9.4.7
Standard	Network Routing Control	9.4.8
Standard	Security of Network Services	9.4.9
Policy	Operating System Access Control	9.5
Standard	Automatic Terminal Identification	9.5.1
Standard	Terminal Log-On Procedures	9.5.2
Standard	User Identification and Authentication	9.5.3
Standard	Password Management System	9.5.4
Standard	Use of System Utilities	9.5.5
Standard	Duress Alarm To Safeguard Users	9.5.6
Standard	Terminal Time-Out	9.5.7
Standard	Limitation of Connection Time	9.5.8

Policy	Application Access Control	9.6
Standard	Information Access Restrictions	9.6.1
Standard	Sensitive System Isolation	9.6.2
Policy	Monitoring System Access and Use	9.7
Standard	Event Logging	9.7.1
Standard	Monitoring System Use	9.7.2
Standard	Clock Synchronisation	9.7.3
Policy	Mobile Computing and Teleworking	9.8
Standard	Mobile Computing	9.8.1
Standard	Teleworking	9.8.2
Systems Development and Maintenance		10
Policy	Security Requirements of Systems	10.1
Standard	Security Requirements Analysis and Specification	10.1.1
Policy	Security In Application Systems	10.2
Standard	Input Data Validation	10.2.1
Standard	Control of Internal Processing	10.2.2
Standard	Message Authentication	10.2.3
Standard	Output Data Validation	10.2.4
Policy	Cryptographic Controls	10.3
Standard	Policy on the Use of Cryptographic Controls	10.3.1
Standard	Encryption	10.3.2
Standard	Digital Signatures	10.3.3
Standard	Non-Repudiation Services	10.3.4
Standard	Key Management	10.3.5
Policy	Security of System Files	10.4
Standard	Control of Operational Software	10.4.1
Standard	Protection of System Test Data	10.4.2
Standard	Access Control to Program Source Library	10.4.3
Policy	Security in Development and Support Processes	10.5
Standard	Change Control Procedures	10.5.1
Standard	Technical Review of Operating System Changes	10.5.2
Standard	Restrictions on Changes to Software Packages	10.5.3
Standard	Covert Channels and Trojan Code	10.5.4
Standard	Outsourced Software Development	10.5.5
Business Continuity Planning		11
Policy	Aspects of Business Continuity Management	11.1
Standard	Business Continuity Management Process	11.1.1
Standard	Business Continuity and Impact Analysis	11.1.2
Standard	Writing and Implementing Continuity Plans	11.1.3
Standard	Business Continuity Planning Framework	11.1.4
Standard	"Testing, Maintaining and Re-assessing Business Continuity Plans"	11.1.5

Compliance		12
Policy	Compliance with Legal Requirements	12.1
Standard	Identification of Applicable Legislation	12.1.1
Standard	Intellectual Property Rights (IPR)	12.1.2
Standard	Safeguarding of Organisational Records	12.1.3
Standard	Data Protection and Privacy of Personal Information	12.1.4
Standard	Prevention of Misuse of Information Processing Facilities	12.1.5
Standard	Regulation of Cryptographic Controls	12.1.6
Standard	Collection of Evidence	12.1.7
Policy	Reviews of Security Policy and Technical Compliance	12.2
Standard	Compliance with Security Policy	12.2.1
Standard	Technical Compliance Checking	12.2.2
Policy	System Audit Considerations	12.3
Standard	System Audit Controls	12.3.1
Standard	Protection of System Audit Tools	12.3.2