



Privacy Confidentiality

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_P4.2_Privacy_Confidentiality.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	Unauthorized 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	Unauthorized 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	Unauthorized 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 Policy Statement.....	5
2. IMPLEMENTATION.....	5
3. REFERENCES AND LINKS.....	5

CTO/P4.2 SECURITY - PRIVACY AND CONFIDENTIALITY

Government Policy on Information & Communication Technology

CTO/P4.2 Security - Privacy and Confidentiality

Security Classification:	Public	Version:	V2.3.1	Status:	Approved
Audience:	SA Government Agencies	Compliance:	Mandatory		
Mandate/Authority:	Chief Technology Officer	Creator:	Government ICT Services		
Authorisation Date:	13 May 1996	Primary Contact:	Strategy & Operations		
Last updated:	16 December 2003		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 1998, 2004, 2007
[Disclaimer](#)
This page was last modified 12 May 2004

1. BACKGROUND

1.1 Policy Statement

Privacy and Confidentiality of Government data is governed by Cabinet Circular Number: 12 (Cabinet Administrative Instruction 1/89) titled Information Privacy Principles.

2. IMPLEMENTATION

1. As part of a data management plan, each agency must define authorised access for all its data - who has access, authority required, level of access allowed.
2. "Authorised access" is defined as access to, use of, copying of, or any form of communication with the data owned by an agency.

3. REFERENCES AND LINKS

1. Cabinet Circular Number: 12 (Cabinet Administrative Instruction 1/89) titled Information Privacy Principles.
2. CTO/P3.1 Government Policy on Information & Communication Technology - Data and Information - Custodianship.
3. CTO/P3.3 Government Policy on Information & Communication Technology - Data and Information – Ownership in an Outsourced Environment.
4. CTO/P4.1 Government Policy on Information & Communication Technology – Security – Information Security Management Framework.
5. South Australian Government Information & Communication Technology Security Guidelines.