



Ownership in an Outsourced Environment

Confidentiality: Public

Prepared By:

Version:

Date: 11 July 2005

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\Data and Information\revised\CTO_P3.3_Ownership_Outourced_Environment.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
DATA AND INFORMATION - OWNERSHIP IN AN OUTSOURCED ENVIRONMENT	4
1. BACKGROUND	5
1.1 Policy Statement	5
1.2 Rationale & Background.....	5
2. IMPLEMENTATION.....	5
3. REFERENCES AND LINKS	6

CTO/P3.3 DATA AND INFORMATION - OWNERSHIP IN AN OUTSOURCED ENVIRONMENT

Government Policy on Information & Communication Technology

CTO/P3.3 Data and Information - Ownership in an Outsourced Environment

Security Classification:	Public	Version:	V3.3.F	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 Reviewed:	10 May 2007		Government ICT Services Division		
Expiry Date:	30 June 2007		Department for Transport, Energy and Infrastructure		
Publication Date:	15 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 11 July 2005

1. BACKGROUND

1.1 Policy Statement

Where an external provider (the Provider) delivers Information Technology services to Government, Government retains ownership of the data or information that is related to the services delivered by the Provider, or which becomes known or available to the Provider. Though the Government data may be resident on the Provider's equipment, they have no rights concerning Government information or data unless such rights are specifically conferred by Government.

1.2 Rationale & Background

1. This policy reinforces Agency obligations identified in three other Government Policies on Information & Communication Technology, being:
 - **Government Policy on Information & Communication Technology – CTO/P3.1 Data and Information - Custodianship:** Even though data storage and management may transfer to a Provider, obligations as specified in the policy on custodianship must still be carried out. Continued ownership of the data (and its attendant custodianship) obliges the contracting Agency (Agencies) to ensure that the obligations are carried through.
 - **Government Policy on Information & Communication Technology – CTO/P1.3 Governance - Intellectual Property Rights:** Continued Government ownership of data in an outsourced environment safeguards the Governments data-ownership interests.
 - **Government Policy on Information & Communication Technology – CTO/P4.2 Security - Privacy and Confidentiality:** Continued ownership of data obliges the contracting Agency (Agencies) to monitor adherence to its obligations of confidentiality of data.

2. IMPLEMENTATION

1. In any outsourcing arrangement, Agencies must ensure that the Providers are aware of Government's continuing ownership of its data.
2. If the Provider is also designated as the custodian, the Agency (Agencies) responsible for transfer must ensure that the Provider enacts and monitors arrangements to adhere to the Government information technology policies outlined in the References above (and any other policies which identify obligations arising from data custodianship).

3. REFERENCES AND LINKS

1. CTO/P1.3 Government Policies on Information & Communication Technology - Governance - Intellectual Property Rights
2. CTO/P3.1 Government Policies on Information & Communication Technology - Data and Information – Custodianship
3. CTO/P4.2 Government Policies on Information & Communication Technology - Security - Privacy and Confidentiality