



## Security - Outsourced Environment

**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\_P4.3\_Security\_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

<b>TABLE OF CONTENTS .....</b>	<b>3</b>
<b>1. BACKGROUND .....</b>	<b>5</b>
<b>1.1 Policy Statement .....</b>	<b>5</b>
<b>1.2 Rationale &amp; Background .....</b>	<b>5</b>
<b>2. IMPLEMENTATION.....</b>	<b>5</b>
<b>3. REFERENCES AND LINKS .....</b>	<b>6</b>

## CTO/P4.3 SECURITY - SECURITY IN AN OUTSOURCED ENVIRONMENT

### Government Policy on Information & Communication Technology

#### CTO/P4.3 Security - Security in an Outsourced Environment

---

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

Contracts with external service providers must specify agency-approved information security policies and procedures and must contain provisions to indemnify the South Australian Government and its agencies against the outcomes of violations to the policies and procedures. While the service provider is the data steward, the Government continues to own the data and the agency retains the responsibility of custodianship of the data.

### 1.2 Rationale & Background

1. As the owner of its data, Government is obliged to ensure that the data-steward in an outsourced environment meets the obligations of the Government Policy on Information Technology - Data and Information - Security and the obligations and principles laid out in Premier and Cabinet Circular no. 12.

## 2. IMPLEMENTATION

1. A data steward is a non-Government person or organisation who is entrusted with the management of Government data.
2. The outsourcing contract must:
  - Identify the obligations of the data steward to prevent a breach of security occurring, in line with the standards specified in the S.A. Government Information Technology Security Standards - In an Outsourced Environment.
  - Provide remedies for the South Australian Government in the event of damage to assets belonging to the Government and the unauthorised access to, use of, or release of information which relates to:
    - the enforcement of a law of the Commonwealth or of a State or Territory
    - the personal affairs of any person
    - the protection of public safety
    - trade secrets and commercial information the disclosure of which could cause advantage or disadvantage to any person
    - any other information that would be exempted under the Freedom of Information Act 1992 from release.

### **3. REFERENCES AND LINKS**

1. CTO/P4.1 Government Policy on Information & Communication Technology – Security – Information Security Management Framework
2. CTO/P4.4 Government Policy on Information & Communication Technology – Security – Security Violations
3. Premier and Cabinet Circular no. 12, Information Privacy Instruction.