



# Protection of Intellectual Property Rights

**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\Data and Information\revised\CTO\_P3.4\_Protection\_Intellectual\_Property\_Rights.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>DATA AND INFORMATION - PROTECTION OF INTELLECTUAL PROPERTY RIGHTS.....</b>	<b>4</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/P3.4 DATA AND INFORMATION - PROTECTION OF INTELLECTUAL PROPERTY RIGHTS

### Government Policy on Information & Communication Technology

#### CTO/P3.4 Data and Information - Protection of Intellectual Property Rights

---

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 Reviewed:	10 May 2007		Government ICT Services Division		
Expiry Date:	31 December 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 12 May 2004

---

## **1. BACKGROUND**

### **1.1 Policy Statement**

Government agencies must take appropriate steps to protect the Government right of Intellectual Property over its data.

### **1.2 Rationale & Background**

1. Agencies must exercise ownership over their data in order to:
  - ensure adequate levels of confidentiality and security
  - control the extent and type of use of the data
  - control the liability which might attach to use of the information
  - obtain a return on the information where appropriate
  - ensure that the information is maintained to a suitable standard
2. Agencies need to have in place appropriate mechanisms to protect the investment Government has made in acquiring and maintaining its data to ensure that its service delivery and economic development goals can be met.

## **2. IMPLEMENTATION**

1. Intellectual Property occurs when an individual or organisation produces original material or intangibles, or enhances material or intangibles which originate elsewhere. Intellectual property is protected under statute law through copyright, patents, trademark and design legislation.
2. There will be circumstances in which third parties such as contractors may be entitled to hold intellectual property rights in respect of Government data they have collected. In these situations, agencies must negotiate Government's intellectual property rights over the data.
3. Common methods of protecting Government data are limiting access to the data, use of the Copyright Act, and the negotiation of data licences with those who use Government data.
4. Though limiting access to data is one method of protecting Government's intellectual property rights, this must be balanced with the requisite for open government inherent in the Government Policy on Information Technology - Data and Information - Availability.

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

1. CTO/P3.1 Government Policy on Information & Communication Technology - Data and Information - Custodianship
2. CTO/P3.2 Government Policy on Information & Communication Technology - Data and Information - Availability
3. CTO/P4.1 Government Policy on Information & Communication Technology – Security – Information Security Management Framework
4. CTO/P4.2 Government Policy on Information & Communication Technology – Security – Privacy and Confidentiality
5. Data Licence available from Crown Solicitor's Office.