



Software Asset Compliance

Confidentiality: Public
Prepared By: Business Unit
Version: Version No
Date: 22 January 2007

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

Signature:

Date Approved:

Document Control

Document Location

Document2

Electronic Records Management Information

File Folder Number: File Folder No – Document Number: Document No

Author(s)

Function / Role

Author

Role

Revision by

Version

Date

Initial draft and consultation

Version No

Distributed to

Version

Date

Confidentiality Classification Table

	Confidentiality	Description	Circulation Limit (on a "NEED TO KNOW" basis)
	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.
	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.
	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.
	Unclassified	No special classification is assigned.	No special restrictions other than legislative or administrative requirements.
	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	7
1.1 Policy Intent/Purpose	7
1.2 History	7
1.3 Policy Intent/Purpose	7
1.4 Policy Audience	7
1.5 Considerations	7
2. SCOPE.....	8
2.1 Policy Statement	8
3. LINKED DOCUMENTS	8
4. MANAGEMENT RESPONSIBILITIES	8
5. EMPLOYEE RESPONSIBILITIES	8
5.1 Executive Director Approval	8
ATTACHMENT 1: FACT SHEET - US FREE TRADE AGREEMENT IMPLEMENTATION ACT 2004.....	9
Background.....	9
Broadening the scope of existing offences	9
New offence relating to significant infringement of copyright....	10
Where to get further information.....	10

CTO/P 2.6 Sourcing – Software Asset Compliance

Government Policy on Information & Communication Technology

CTO/P 2.6 Sourcing – Software Asset Compliance

Security Classification:	Public	Version:	1.0	Status:	Approved
Audience:	Government Agency CIO	Compliance:	Mandatory		
Mandate/Authority:	Chief Technology Officer	Creator:	Government ICT Services		
Authorisation Date:	22 January 2007	Primary Contact:	Strategy & Operations		
Last updated:	October 2006		Government ICT Services Division		
Expiry Date:	February 2010		Department for Transport, Energy and Infrastructure		
Publication Date:	9 February 2007		Tel: 8226 3558		

Coverage:

The South Australian public authorities required to adhere to this Policy 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 his or her 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 2006
[Disclaimer](#)
This page was last modified October 2006

Document Location:**File Name and Path of Master Document**

Q:\Strategy & Innovation\Policy & Standards Project\Policies on the web\04 Sourcing\Policies\Updated versions\CTO_P2.6_Software_Asset_Compliance.doc

Author(s):

Name	Function
Denise Curnow	Senior Project Officer

Revision History:

Version	Revision Description	Date
0.01	Reviewed by Cathy Johnson – Manager Integration & Compliance and Daryl Keen – Manager Program Office	3/7/06
0.02	Andrew Jones, Manager Strategy & Standards & Michelle O'Day - Project Officer Strategy & Standards	3/8/06
0.03	Reviewed by Cathy Johnson, Manager Integration & Compliance	21/8/06
0.04	GovtICT Executives and CTO Reference Group	October 2006
1.0	Mike Grillo, Chief Technology Officer	22/1/2007

Distribution List:

Distributed to	Title	Date
All GICTS Executive	Operational Executives	October 2006
All CTO Reference Group Members	CTO Reference Group	October 2006
Mike Grillo	Chief Technology Officer	January 2007

Confidentiality Classification:

	Confidentiality	Description	Circulation Limit
	X-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 access within SA Government and to authorised industry partners only
	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

Approval:

Name	Title	Signature	Date
Mike Grillo	Chief Technology Officer & Executive Director, Government ICT Services		

TABLE OF CONTENTS

TABLE OF CONTENTS	6
BACKGROUND	7
Policy Intent/Purpose	7
History	7
Policy Intent/Purpose	7
Policy Audience.....	7
Considerations	7
SCOPE	8
Policy Statement	8
LINKED DOCUMENTS	8
MANAGEMENT RESPONSIBILITIES.....	8
EMPLOYEE RESPONSIBILITIES.....	8
Executive Director Approval.....	8
ATTACHMENT 1: FACT SHEET - US FREE TRADE AGREEMENT IMPLEMENTATION ACT 2004.....	9

1. BACKGROUND

1.1 Policy Intent/Purpose

The *US Free Trade Agreement Implementation Act 2004* (USFTAI Act) and *Copyright Legislation Amendment Act 2004* (CLA Act) as of 1 January 2004 made a series of amendments to criminal offence provisions of the *Copyright Act 1968*.

A key obligation referenced under the Amendments is the provision of information regarding to criminal proceedings and penalties to individual/s and can be applied **at least** in cases of wilful copyright piracy on a commercial scale (including Government organisations).

See US Free Trade Agreement Implementation Act 2004 fact sheet - **Attachment 1**.

1.2 History

The Office of the CTO is accountable for ensuring observance and attainment of the Government's ICT compliance. To prove compliance Authorities and in particular responsible individuals will be accountable for producing an electronic report against specified criteria on a regular basis.

1.3 Policy Intent/Purpose

The intent and purpose of this policy is to ensure compliant authorities adhere to software asset compliance and realise the benefits of software asset management methodologies and compliance standards, which are measured in various ways across Government.

1.4 Policy Audience

Each South Australian Government compliant authority (as defined in CTO/P1.1 Government Policy on Information & Communication Technology – Governance – Compliant Authorities.)

1.5 Considerations

Portfolios have differing IT networks and infrastructure that are not necessarily centrally managed. Several Agencies consider themselves not part of an overall Portfolio to which they are aligned, therefore utilise separate infrastructure, procurement processes and work autonomously. Thought needs to be given by the overall Portfolios when reporting software compliance to satisfy CTO responsibilities.

Those lead agencies working independently are required to report their compliance whether they have an electronic or manual system for managing their software assets. Having an internal Software Asset Management work group per Portfolio to communicate and coordinate across their entire Portfolio and work towards a centralised approach across the State would be beneficial.

2. SCOPE

The SAM policy encompasses the management of all software assets and their compliance to current software licencing arrangements across government's compliant authorities. The knowledge of what software assets have been procured, usage of these assets and the ability to prove compliance across government at any given time supports the State's position of strength and advantage when dealing with future contract negotiations with vendors.

2.1 Policy Statement

Each South Australian Government instrumentality will:

- Comply with licensing agreements and conditions regarding software licences (software assets) owned and utilised by South Australian Government;
- Maintain evidence of software licensing compliance; and
- Complete the CTO's quarterly software compliance report with supporting evidence demonstrating asset compliance.

3. LINKED DOCUMENTS

- CTO/P1.1 Government Policy on Information & Communication Technology – Governance – Compliant Authorities.
- Compliance Management Framework.

4. MANAGEMENT RESPONSIBILITIES

- The Chief Technology Officer (CTO) has responsibility for software compliance assurance for the State Government.
- Portfolio Chief Executives (CE) or Lead Agency equivalents have responsibility for ensuring the compliance of their organisation regarding software assets, their compliance and adherence to this policy.

5. EMPLOYEE RESPONSIBILITIES

Responsibilities for software asset compliance lie within each Portfolio / Agency instrumentality and individual employees. All employees have a responsibility under their "Code of Conduct" regarding adherence to the regulations of software asset compliance.

5.1 Executive Director Approval

Mike Grillo,
Executive Director and Government Chief Technology Officer,
Government ICT Services,
Department for Transport, Energy and Infrastructure

ATTACHMENT 1: FACT SHEET - US FREE TRADE AGREEMENT IMPLEMENTATION ACT 2004

AMENDMENTS TO CRIMINAL LAW PROVISIONS OF *COPYRIGHT ACT 1968* TO IMPLEMENT OBLIGATIONS IN AUSTRALIA-UNITED STATES FREE TRADE AGREEMENT

Background

The *US Free Trade Agreement Implementation Act 2004* (USFTAI Act) and the *Copyright Legislation Amendment Act 2004* (CLA Act) made a series of amendments to criminal offence provisions of the *Copyright Act 1968* (the Act). The amendments implement general criminal law obligations under the Australia-United States Free Trade Agreement (AUSFTA). Both the AUSFTA and the criminal law offence amendments in the USFTAI Act and the CLA Act came into force on 1 January 2005.

The key criminal offence obligation under the AUSFTA is to provide for criminal procedures and penalties to be applied at least in cases of wilful copyright piracy on a commercial scale.

Under the AUSFTA, this includes two specific types of conduct:

(1) Where a person has committed significant wilful infringements of copyright with no direct or indirect motivation of financial gain.

(2) Where a person has committed wilful infringements of copyright for the purposes of commercial advantage or financial gain.

Implementation of this obligation has been achieved by a series of amendments to the criminal law provisions in sections 132 (general offences) and 135AS (broadcast decoding devices) of the Act.

Broadening the scope of existing offences

The amendments made by the USFTAI Act and the CLA Act will broaden the scope of offences in sections 132 and 135AS of the Act to criminalise certain activity involving infringing copies and broadcast decoding devices where that activity is committed 'with the intention of obtaining a commercial advantage or profit'. For example, the distribution from an Internet site of infringing copies of movies or computer software not for profit but for some other commercial advantage (e.g., attracting commercial sponsorship) may come within the scope of the offence.

The amendments will also broaden the scope of the offence in paragraph 132(1)(a) of the Act so that it applies to the making of infringing copies with the intention of obtaining a commercial advantage or profit (thereby strengthening the current offences regime that targets activity such as 'business end user piracy'). For example, this will ensure that the offence is wide enough in scope to criminalise the making of infringing copies of computer software in a business for internal commercial use.

Importantly, the amendments include a definition of 'profit', which excludes 'any advantage, benefit or gain resulting from or associated with private or domestic use of any copyright material in the work or other subject-matter'. This ensures that the scope of the offences does not extend beyond commercial uses of copyright material in a work or other subject matter.

New offence relating to significant infringement of copyright

The amendments also inserted new subsection 132(5DB) into the Act, which makes it an offence where:

- a person has committed one or more infringements of the copyright in a work or other subject-matter,
- the infringement or infringements occur on a commercial scale, and
- the infringement or infringements have a substantial prejudicial impact on the owner of the copyright.

The offence is intended to implement the obligation under the AUSFTA that criminal procedures and remedies apply to a person who has engaged in significant infringing activity on a commercial scale but where they have no direct or indirect motivation of financial gain. For example, this offence may be committed by a person who creates a web site that allows infringing copies of movies or computer software to be downloaded to Internet users for free.

Under new subsection 132(5DC) of the Act, certain matters are to be taken into account in determining whether one or more infringements on a commercial scale under subsection 132(5DB) occurs. These include the volume and value of any articles that are infringing copies.

Other fact sheets outline specific criminal law changes to other areas of the Act, including further changes to provisions dealing with broadcast decoding devices.

Where to get further information

For copies of the USFTAI Act and the CLA Act (and Explanatory Memoranda) visit:
www.comlaw.gov.au

If you would like more information on copyright generally visit
<http://www.ag.gov.au/copyright>, or subscribe to the Attorney-General's Department's
Copyright E-news at <http://www.ag.gov.au/www/eneWSCopyrightHome.nsf>