



Application Guidelines for Exemption from ICT Contracts (2)

Confidentiality: Public
Prepared By:
Version:
Date: 21 November 2007

Approver's Name: Grantley Mailles
Title: Chief Information Officer and
Acting Chief technical Officer

Signature:

Date Approved:

Document Control

Document Location

Q:\General Share Drive\Web updates\post to new site\Governance\revised\CTO_G1.5_Applications_guidelines_Exemption_ICT_Contracts(2).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
Governance - Application Guidelines	4
1. BACKGROUND	6
1.1 History	6
1.2 Policy Intent/Purpose	6
1.3 Audience	6
2. SCOPE.....	6
3. POLICY STATEMENT	6
3.1 Application Process	6
3.1.1 <i>Application to the Chief Information Officer (CIO).....</i>	<i>7</i>
3.1.2 <i>Assessment of Application</i>	<i>7</i>
3.2 Appeal Process	8
4. MANAGEMENT RESPONSIBILITIES	8
5. REFERENCES & LINKS.....	8

CTO/G 1.5

1. Governance - Application Guidelines FOR ELIGIBLE ENTITIES TO APPLY FOR EXEMPTION TO ICT INFRASTRUCTURE CONTRACTS

Government Guideline on Information & Communication Technology

CTO/G 1.5

Governance - Application Guidelines for Eligible Entities to Apply for Exemption to ICT Infrastructure Contracts

Security Classification:	Public	Version:	1.4	Status:	Approved
--------------------------	--------	----------	-----	---------	----------

Audience:	SA Government	Compliance:	Mandatory
Mandate/Authority:	Chief Technology Officer	Creator:	Office of the CIO
Authorisation Date:	29 June 2006	Primary Contact:	Governance & Investment Office of the Chief Information Officer
Last updated:	20 November 2007		Tel: 8226 5998
Review Date:	30 December 2008		
Publication Date:	21 November 2007		

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 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 2006, 2007

[Disclaimer](#)

This page was last modified November 2007

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

Q:\Strategy & Innovation\Strategy and Standards\Policies Standards and Guidelines\Guidelines\03 Governance\CTO_G1 5_Application_Guidelines_Exemption_ICT_Contracts (2).doc

Author(s):

Name	Function
Integration & Compliance	Office of the CIO

Revision History:

Version	Revision Description	Date
0.0.1	First Draft	6 April 2006
1.0.0	Updated after internal consultation	10 April 2006
1.0.1	Updated following feedback	May 2006
1.3.1	Endorsement by FICT Steering Committee	29 June 2006
1.4	Minor procedural change	12 November 2007

Distribution List:

Distributed to	Version	Date
Future ICT Steering Committee	1.0.1	May 2006

Confidentiality Classification Table:

	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
Grantley Mailles (per Andrew Jones)	Chief Information Officer and A/Chief Technology Officer	Original signed.	21 November 2007

1. BACKGROUND

1.1 History

This guideline was created following requests from various sources for a comprehensive summary of the steps to be followed to apply for exemption from ICT Infrastructure contracts. It is intended to formalise various ad hoc instructions previously available.

1.2 Policy Intent/Purpose

The Application Guidelines is a definitive collection of the steps, which must be followed by any entity seeking exemption from an ICT Infrastructure contract. The guidelines are intended to ensure any such entity has fully considered the ramifications of an exemption, and followed a consistent process in lodging an application. The guidelines also outline the appeal process, which can be followed if the original application is rejected.

1.3 Audience

The audience for this policy is any entity, which is eligible to access the South Australian Information Communication Technology (ICT) Strategic Sourcing Service Contracts.

2. SCOPE

The Application Guidelines:

- Describe the information to be provided by an entity seeking an exemption;
- Define the factors to be considered when a determination is made in regards to an application outlining the appeal process; and
- Details the role of the applying entity and of the Office of the Chief Information Officer.

3. POLICY STATEMENT

3.1 Application Process

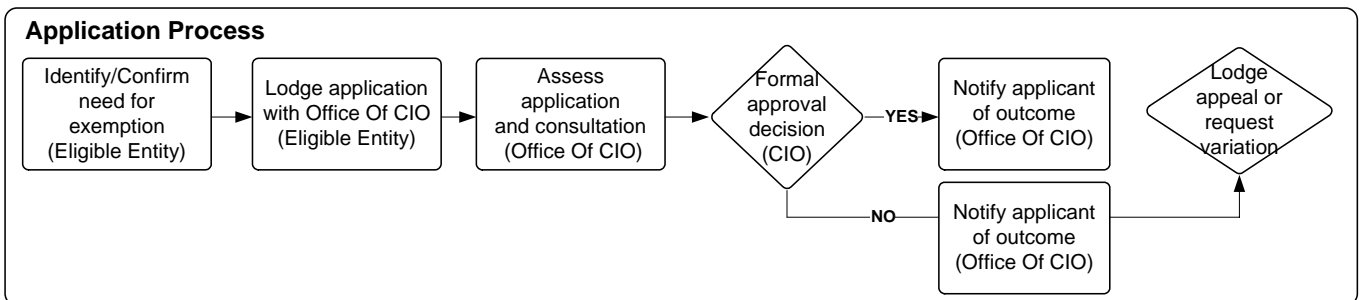


Figure 1: Application for exemption from ICT infrastructure contracts process

3.1.1 *Application to the Chief Information Officer (CIO)*

Eligible entities can apply for exemption from using the ICT infrastructure contracts for specific components by completing an *Exemptions On-Line* application. The application requires agencies to address the following issues:

- What contracts the exemption covers (eg Electronic Messaging, Mainframe etc);
- What components the application for exemption covers (describe in sufficient detail to define where the boundary of exemption is, including a statement of how the system/application is connected to the State's Data Network);
- The reasons/ justifications for the exemption request;
- Proposed term of the exemption (NB maximum period of exemption is the term of the contract);
- The contact details for further information regarding the application; and
- Current contractual arrangements and proposed alternative arrangements.

Supplying all these details and any other information considered to be important will allow a faster assessment by the Office of the Chief Information Officer (CIO).

The application must be authorised by the **appropriate agency delegate** (CIO/CTO) before it can be assessed by the OCIO.

The on line application and instructions for use are available by linking to the following: [Exemptions On-Line](#).

3.1.2 *Assessment of Application*

Following assessment of this application from the Office of the CIO, the CIO will approve or otherwise the application and will respond with any conditions stipulated for the exemption.

After receiving the application, it is expected that the Office of the CIO will be able to deliver a decision within 15 working days, depending on the complexity of the request.

The application will be assessed against the following criteria:

- 1) Contractual implications;
- 2) Architectural implications;
- 3) Interoperability considerations;
- 4) Security requirements;
- 5) Operational issues;
- 6) Agency business requirements;
- 7) Business needs being met within existing contract.

3.2 Appeal Process

If a 'not approved' reply is received for the application, an appeal process can be undertaken. This process is shown in figure 2.

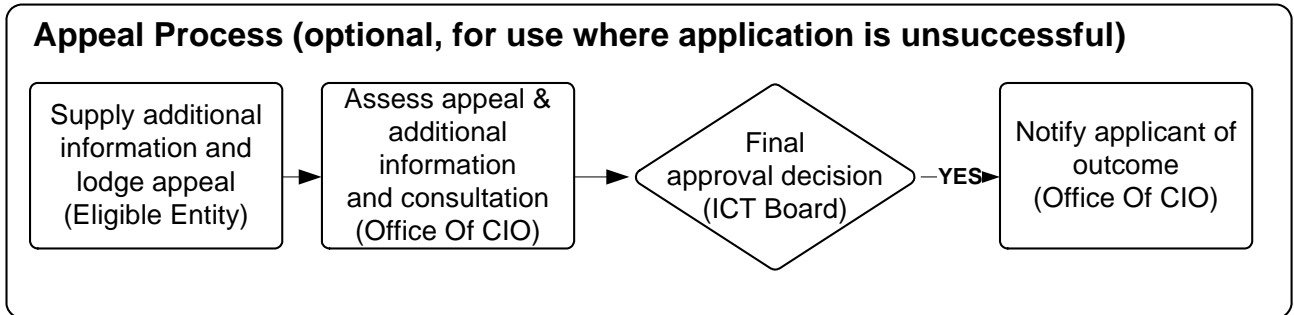


Figure 2 – Appeal process

4. MANAGEMENT RESPONSIBILITIES

Chief Executives are responsible for ensuring the compliance of their organisations with this policy.

5. REFERENCES & LINKS

CTO/P1.1 Governance – Compliant Authorities

CTO/P1.2 Governance – Exemptions

CTO/S1.1 Governance - Procedure For Exemption From Mandated Application Software

CTO/P2.1 Sourcing – Information Technology Infrastructure Services