



Government Domains

Confidentiality: Public

Prepared By:

Version:

Date: 4 April 2007

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\Applications and Internet\revised\CTO_P5.3_Government_Domains.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

0.1

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
CTO/P5.3 APPLICATIONS – INTERNET - GOVERNMENT DOMAINS	4
1. BACKGROUND	6
1.1 Policy History.....	6
1.2 Intent/Purpose	6
2. SCOPE.....	6
2.1 Scope Exclusions.....	6
3. POLICY	7
3.1 Policy Exemptions	7
4. ACCOUNTABILITIES & AUTHORITIES.....	7

CTO/P5.3 APPLICATIONS – INTERNET - GOVERNMENT DOMAINS

Government Policy on Information & Communication Technology

CTO/P5.3 Applications – Internet – Government Domains

Security Classification:	Public	Version:	V1.0	Status:	Approved
--------------------------	--------	----------	------	---------	----------

Audience:	SA Government	Compliance:	Mandatory
Mandate/Authority:	Chief Technology Officer	Creator:	Government ICT Services
Authorisation Date:	4 April 2007	Primary Contact:	Government ICT Services
Last updated:	February 2007		Department for Transport, Energy and Infrastructure
Expiry Date:	February 2009		Tel: 8226 3558
Publication Date:	April 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 2007

[Disclaimer](#)

This page was last modified on 6 February 2007

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

Q:\Strategy & Innovation\Policies_Standards_Guidelines\Policies\07 Applications and Internet\ CTO_P5.3_Government_Domains.doc

Author(s):

Name	Function
Service Delivery Group	

Revision History:

Version	Revision Description	Date
0.1	Draft working document	2 November 2006
0.2	Minor changes	27 February 2007
1.0	Approved version	4 April 2007

Distribution List:

Distributed to	Title	Date
CTO Reference Group		27 February 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	Original signed	4 April 2007

1. BACKGROUND

This document describes the policy appropriate for the management of internal and external Domains used by the South Australian Government (SAG) and Local Government.

Domains used as a naming convention by people to access web applications (e.g. www.xyz.sa.gov.au), where “xyz.sa.gov.au” is a *unique* and *appropriate* domain name. It is important that all domain names are unique to ensure that computers are able to locate the required web application. It is important that the name be appropriate to ensure the good name of the South Australian Government is not inadvertently brought into disrepute and (preferably) that the name is sufficiently descriptive to provide an indication of the application’s purpose.

To maintain the uniqueness and appropriateness, Government Domains are managed centrally. Within Australia, the Australian Government Information Management Office (AGIMO), is the *approving authority* for requests associated with the “.gov.au” Domain.

In South Australia, the approving authority for requests associated with the “.sa.gov.au” Domain is Government ICT Services.

1.1 Policy History

This is a new policy.

1.2 Intent/Purpose

The intent of this document is to ensure that domain names used in accessing SAG applications are *unique* and *appropriate* whether within the SAG network or the Internet.

2. SCOPE

This policy applies to any Compliant Authority as defined in *GICT/P1.1 Government Policy on Information & Communication Technology – Governance – Compliant Authorities* namely:

- State Government Agencies
- Statutory Authorities
- Local Government.

2.1 Scope Exclusions

The following matters are excluded from the scope:

- Domain names used by non-Government entities.

3. POLICY

1. The creation, use and management of Government Domain Names will be appropriate in maintaining or enhancing the image of the SA Government;
2. Any requests for, or changes associated with the '**.sa.gov.au**' Domain require the prior approval of the approving authority (Government ICT Services);
3. Only one domain name will be used per website unless there is a legitimate reason to do otherwise. Exceptions to this policy rule may be granted by the Approval Authority.

3.1 Policy Exemptions

Compliant Authorities seeking exemption from this policy are referred to *CTO/P1.2 Governance – Exemptions (see also section 4)*.

4. ACCOUNTABILITIES & AUTHORITIES

The Executive Director, Government ICT Services is delegated as the Approval Authority for Domains associated with the '*.sa.gov.au*' Domain.

Departmental Chief Executives hold the authority for determination of other Domain Names used by a Compliant Authority within their delegation.