Government of South Australia

DPC/P7.4

ACROSS GOVERNMENT POLICY

Acceptable Use Policy - Guest Network

Purpose

The primary purpose for which the South Australian (SA) Government provides relevant users with access to the guest network is to assist them in carrying out their duties within a public sector agency. The SA Government's intention for publishing this Acceptable Use Policy is not to impose restrictions that are contrary to the SA Government's established culture of openness, trust and integrity. It recognises that the guest network is an important asset to the SA Government and must be managed with care. Its use must be ethical, lawful and appropriate, in accordance with the SA Government's values and policies, and with any applicable State and Commonwealth legislation and regulations.

Scope

This policy applies equally to

- All full-time, part-time, and temporary public sector employees
- All contractors engaged by the agency; and
- All third parties providing services to the agency.

This policy applies to all equipment connected to the SA Government guest network.

Background

The SA Government is committed to protecting its employees, partners and agencies from illegal or damaging actions by individuals, either knowingly or unknowingly.

Effective security is a team effort involving the participation and support of every user who deals with information and/or information assets (IT assets). It is the responsibility of every user to know the requirements under this policy and to conduct their activities accordingly in a responsible manner.

This policy encompasses all users and governs the common principles behind the use of assets. These rules are in place to protect the user and the SA Government. Inappropriate use exposes the SA Government to risks including virus attacks, compromise of network systems and services, and legal issues.

Policy detail

General Use and Ownership

While the SA Government's network administration aims to provide a reasonable level of privacy, users should be aware that the data traversed across or transmitted over the guest network might be inspected when required. Management cannot guarantee the confidentiality of information because of the need to protect the SA Government.

Users are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of guest / Internet / Intranet and Extranet systems. In the absence of such policies and guidelines, users should be guided by departmental policies on personal use, and if there is any uncertainty, users should consult their supervisor or manager.

The SA Government recommends that any information that users consider sensitive or vulnerable be encrypted while using the guest network.

For security and network maintenance purposes, authorised individuals may monitor equipment, systems and network traffic at any time.

The SA Government reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

All records, transactions, emails, instant messages, internet access and other activity logs are discoverable under the *Freedom of Information Act 1991*, *Evidence Act 1929* and *Electronic Communications Act 2000*.

Security

All hosts used by the user that are connected to the SA Government guest network, whether owned by the user or the SA Government, shall be continually executing approved virus-scanning software with a current virus database, unless overridden by a departmental or group policy.

Unacceptable Use

The following activities are, in general, prohibited. Users may be exempted from these restrictions during their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is a user authorised to engage in any activity that is illegal under local, state, commonwealth or international law while using the guest network resources.

The list below is by no means exhaustive but attempts to provide examples of activities that fall into the unacceptable use category.

System and Network Activities

The following activities are strictly prohibited, with no exceptions:

- Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the downloading or distribution of "pirated" or other software products that are not appropriately licensed for use by the SA Government.
- Unauthorised copying of copyrighted material including, but not limited to, digitisation and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which the end user does not have an active license is strictly prohibited.
- Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws.
- Knowingly introducing malicious programs into the network or server environment (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
- Conducting private business, for personal gain, or to operate or maintain a personal website.
- Accessing, procuring, downloading, displaying, transmitting or publishing on or over the guest network, any information of an obscene or profane nature, or material likely to be sexually offensive to an average person or contrary to generally accepted social standards. Clear examples of such material include but are not limited to:
  - Materials that contain sexually explicit images or descriptions.
  - Materials that advocate illegal activity.
  - Materials that advocate intolerance or hatred for others; and
  - Materials that are bullying or harassing in any way.
- Transmitting, or causing to be transmitted, communication that will be construed as harassment or disparagement of others based on the criteria of any antidiscrimination legislation.
- Publishing on or over the guest network any information which violates or infringes upon the rights of any other person or group, including material of an abusive nature.
- Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to:
  - accessing data of which the employee is not an intended recipient; and

    - logging into a server or account that the user is not expressly authorised to access.
- For purposes of this section, "disruption" includes, but is not limited to:
    - network sniffing or reconnaissance activity
    - ping floods
    - packet spoofing
    - denial of service
    - forged routing information for malicious purposes
- Port scanning or security scanning.
- Executing any form of network monitoring that will intercept data not intended for the user of the guest network.
- Seeking to gain or gaining unauthorised access to information systems, resources or entities.
- Interfering with or denying service to cause severe degrades or disrupt IT assets' performance (for example, denial of service attack).
- Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means.
- Participating in gambling activities, but not limited to those provided by the casino and internet-based gaming sites.

<u>Email and Communication Activities</u>

- Sending unsolicited emails to the SA Government, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
- Unauthorised use, or forging, of email header information.
- Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
- The creation or transmission of obscene, defamatory or harassing email or instant messages, as is the distribution of email chain letters, spam or any other material which could be considered annoying, offensive or illegal.
- Posting the same or similar non-business related messages to large numbers of Usenet newsgroups (newsgroup spam).

Enforcement

Any person authorised to use the guest network and found to have violated this policy may result in disciplinary action in accordance with the *Public Sector Act 2009* or the *Code of Ethics for the South Australian Public Sector*, particularly for deliberate policy violations. This may be in addition to any prosecution resulting from offences against state or commonwealth legislation or unlawful activity under common law.

Exemption Management

In the event an exemption is warranted, agencies may seek exemption in accordance with the *Governance Exemptions Policy*.

Aboriginal Impact Statement

The needs and interests of Aboriginal people have been considered in the development of this policy. There is no specific impact on Aboriginal people.

Roles and responsibilities

Position title or unit/team	Listed responsibilities
Chief Executive	Accountable for the effective implementation of, and compliance, with this policy within their agency.
Senior Executives and Directors	Ensure there is a clear direction and commitment for the implementation of this policy within the agency. Ensure that this policy is observed by staff and that business processes support policy requirements.
Team Leaders, Supervisors and Managers	Approve requests for guest access. Ensure users are fully informed of their obligations and responsibilities under this policy and trained where required. Ensure contracts and agreements with third parties require adherence to this policy, where relevant. Take appropriate steps should they become aware of a violation of the policy or the supporting procedures. Ensure that any reporting requirements are met.
Agency IT Security Advisor	Review security impacts of any requests for exemption in alignment with the *DPC Security Compliance Exemption Policy.*
All users	Comply with this policy and any related procedures, and to play an active role in ensuring the compliance of others.
Policy Owner / Contact	Maintain and communicate to key stakeholders the requirements for the acceptable use of the guest network . Review and approve requests for exemption to this policy as recommended by the Agency Information Technology Security Adviser.

Related documents

- *Public Sector Act 2009*
- *Code of Ethics for the South Australian Public Sector*
- *Governance Exemptions Policy*

Definitions

Term	Definition
Guest network	a facility provided to staff and agency-sponsored visitors, both government and non-government, with secure access to the internet using local agency access points
Public sector agency	an internal to government entity, including administrative units, bodies corporate, statutory authorities, and instrumentalities of the Crown, as defined in the *Public Sector Act 2009 (SA)*.
Third parties	any individual, contractor, business partner, or agent not directly employed by a South Australian Government that is engaged by an agency to provide goods/services

DOCUMENT CONTROL

Approved by: Chief Information Officer Steering Committee	
Contact: Leslie Szigeti, Infrastructure Manager	Email: les.szigeti@sa.gov.au
Division: OCIO Infrastructure and Customer Service	Compliance: Mandatory
Version: 1.0	Date of approval: 28/06/2023
Next review date: June 2025	Objective ID: B1496499

Licence