



DPC/P4.43

ACROSS GOVERNMENT POLICY

# Email Usage Policy

## Purpose

This policy outlines the requirements that South Australian Government agencies must follow prior to implementing and/or using electronic mail (email) services. This policy creates a consistent baseline of email security requirements for all South Australian Government public sector agencies within the scope of this policy.

## Scope

This policy applies to any compliant authority as defined in [ICT Policy Statement 1 – Compliant Authorities](#), and all South Australian Government public sector agencies (as defined in the Public Sector Act 2009), herein referred to as 'agencies'.

## Background

The [ICT, Cyber Security and Digital Government Strategy \(2020-2025\)](#) outlines the priority to ensure the South Australian Government is secure and trusted. This priority involves strengthening the South Australian Government's approach to preventing, detecting, and responding to cyber security threats and incidents. This policy provides additional governance to assist in enabling this priority.

## Policy Details

Agencies must adopt appropriate policies, procedures, and practices addressing the following email requirements:

1. Alignment in accordance with the [Code of Ethics](#) for the South Australian Public Sector.
2. Primarily used for business-related purposes. Personal communication is permitted on a limited basis, ensuring it aligns with this policy and does not cause harm or reputational damage to the Government of South Australia and its employees.
3. Usage is subject to the [South Australian Government Intellectual Property Policy](#) and must align to the guiding principles and obligations of that policy.
4. Must be stored in line with the State Records of South Australia General Disposal Schedule or agency Records Disposal Schedule.
5. Apply Protective markings to reflect the highest sensitivity or classification of the subject, body and attachments.
6. Must be classified in accordance with the [South Australian Information Classification System \(ICS\)](#).
7. Email must not be automatically forwarded to a third-party Electronic Mail service.

8. Do not send or receive email from external platforms using the sa.gov.au domain, including sub-domains, that is not in accordance with applicable standards, under this policy.
9. Deploy Sender Policy Framework (SPF), Domain Keys Identified Mail (DKIM), Domain-based Message Authentication, Reporting and Conformance (DMARC) and protective marking checks.
10. Sent and received emails must have mail hygiene applied to reduce the impact of threats to South Australian Government systems.
11. Use protocol that encrypts and delivers mail securely, for both inbound and outbound mail traffic.
12. External access to email must be by a method of authentication that uses two or more authentication factors, to authenticate a single claimant to a single authentication verifier.

## Exemptions

Advice regarding exemptions from this policy is provided in the Government Ruling on Information and Communication Technology titled [ICT Ruling 1 Exemptions](#).

## Roles and responsibilities

Position title or unit/team	Listed responsibilities
Agency chief executives	Must maintain agency policies and procedures consistent with this policy
Agency staff	Must comply with relevant agency policies
Contractors	Comply with relevant contractual requirements

## Related documents

- [ICT Policy Statement 1 – Compliant Authorities](#), South Australian Government
- [Code of Ethics for the South Australian Public Sector](#), South Australian Government
- [Intellectual Property Policy](#), South Australian Government
- [South Australia General Disposal Schedule](#), South Australian Government
- [ICT Guideline 1. Governance – Application for Exemption](#), South Australian Government
- [ICT Policy Statement 4 - Using sa.gov.au as a sending address for external applications](#), South Australian Government
- [Internal and External Domains Sending Mail](#) – South Australian Government

## Implementation and Review

Agencies are responsible for reviewing their existing policies, procedures and practices upon commencement of this policy.

The Chief Executive of the Department of the Premier and Cabinet (DPC) may issue guidelines to assist agencies in interpreting and applying this policy and may review any agency policies,

procedures or practices to ensure consistency with this policy. DPC is responsible for reviewing this policy within 5 years of its implementation.

---

## DOCUMENT CONTROL

Approved by: Ed Reynolds

Title: Director, Cloud Services

Contact person: Frank Contestabile

Telephone: (08) 8429 7055

Division: OCIO Cloud Services

Compliance: Mandatory

Review number: 1.0

Date of approval: 21 September 2022

Next review date: September 2024

Date of review:

---

### Licence



With the exception of the Government of South Australia brand, logos and any images, this work is licensed under a [Creative Commons Attribution \(CC BY\) 4.0 Licence](#). To attribute this material, cite Department of the Premier and Cabinet, Government of South Australia, 2022.