DPC/P4.41

ACROSS GOVERNMENT POLICY

Using sa.gov.au as a sending address for external applications (ICT Policy Statement 4)

Purpose

To outline the appropriate way of sending emails from external platforms using the sa.gov.au domain.

Scope

This policy applies to all South Australian Government agencies using the South Australian Government Email Service (as defined in ICT Policy Statement 1 – Compliant Authorities).

Background

Some SA Government agencies have a need to use external digital platforms, applications or services to send emails (such as email marketing platform Campaign Monitor or event listing website Eventbrite*) and have them look like they come from the sa.gov.au email domain in the “From” field. This alone can expose the SA Government to increased email-based threats or result in legitimate emails being blocked. Furthermore, free online services are often used by malicious actors or criminals and so may be blacklisted by email hygiene filters.

Using a digital platform, application or service with a fixed IP address will ensure the SA Government’s Mimecast email security platform is as effective as possible in preventing cyber threats, while still allowing agencies to send emails using an sa.gov.au address.

Policy detail

When requesting the use of the sa.gov.au domain for external applications (such as Campaign Monitor or Eventbrite*), agencies are required to:

- engage their IT Security Adviser in any request for policy or rule changes in their agency Mimecast tenancy
- ensure any request for policy or rule changes will only be made to their individual agency tenancy in Mimecast (i.e. whole of government rules will only be changed if it is a whole of government service utilised by multiple agencies)
- use a dedicated IP address, if available, ahead of dynamic or shared IP addresses

- cease the use of free services and/or services that introduce an unnecessary risk to an agency or government as a whole (seek advice about this from your agency's IT Security Adviser).

When requesting the use of @sa.gov.au as a sending address for an external application, agencies have three options:

Option 1:
Register a subdomain to be used to send email for the external application, e.g. staffsurvey.sa.gov.au. This provides flexibility as multiple email addresses may be used as part of the domain, e.g. bob.smith@staffsurvey.sa.gov.au.

Option 2:
Request a Mimecast rule bypass for a specific email address. For 'Replies', a specific generic mailbox will need to be created, e.g. staffsurvey@sa.gov.au, which could be used to send email via an external tool. The agency may then elect owners of the mailbox to receive any replies.

Option 3:
Purchase platforms or software that have a dedicated IP address. This is the only option for a system which needs to impersonate many SA Government mailboxes. This should only be used when there is a requirement for an external service to imitate all sa.gov.au mailboxes.

Note: selecting Options 1 or 2 should not negate the option for a dedicated IP. Where a service provider has the option for a dedicated IP address, agencies should use this for additional security.

This policy aims to ensure that any use of the sa.gov.au domain via an external platform or service abides by security best practices to reduce any risk to the government email system, while ensuring government email is delivered securely and effectively via the Mimecast email security gateway.

Roles and responsibilities

The Chief Executive of each South Australian Government agency (as defined in ICT Policy Statement 1 – Compliant Authorities) is accountable for the effective implementation of this policy within the agency.

The Deputy Chief Executives, Executive Directors, Directors and Managers are responsible for ensuring:

- the policy is implemented and observed by staff
- staff are fully informed of their obligations and responsibilities under the policy, and trained where required
- contracts and agreements with service providers require adherence to this policy
- any reporting requirements are met.

Related documents

- ICT Policy Statement 1 – Compliant Authorities
- Personal Information Data Breaches

***Please note – you should speak to your agency's IT Security Adviser for information about using such platforms.**

Document control

ID	DPC/P4.41
Version	1.2
Classification/DLM	Public-I2-A1
Compliance	Mandatory
Original authorisation date	23 April 2019
Last approval date	25 September 2019
Next review date	December 2020

Licence