# All of Government

# Secure Government Email DMARC Deployment Guide

*Issued by*

*Digital Services branch*

Internal Affairs
Te Tari Taiwhenua

New Zealand Government

# Contents

# 1 Document Control

| | |
|---|---|
| **Service Name** | Secure Government Email |
| **Author** | Matt Oliver, Operations Security Specialist, Department of Internal Affairs |
| **Title** | Secure Government Email DMARC Deployment Guide |
| **Date and Version** | 4 November 2025, v1.0 |
| **Index Number** | AoGSD.SGE.Guidance.2025_252 |

# 2 Introduction

The Secure Government Email (SGE) Common Implementation Framework was confirmed late in 2024 with a goal to improve email security standards across the New Zealand Government. This deployment guide compliments the Framework through providing examples on how to deploy Domain-based Message Authentication, Reporting, and Conformance (DMARC) in line with both the framework and to meet the requirements of the New Zealand Information Security Manual (NZISM). It provides configuration examples covering commonly used platforms and configurations but is not an exhaustive guide. It is recommended Agencies without experience in the deployment of email security tools engage with a provider with expertise in this area.
Services are available for Agencies via the Secure Email Management and Administration service in Marketplace Marketplace | Pae Hokohoko — Infrastructure Managed Services catalogue.

# 3 NZISM and SGE Framework requirements for SPF

Chapter 15.2 (Email Infrastructure) of the NZISM requires DMARC be configured across all domains irrespective of those domains use in association with email. It requires Agencies deploy DMARC on all domains with a p=reject policy.

The SGE Framework maps back to the NZISM and requires:

- All domains must have a p=reject DMARC policy.
- DMARC Reports must be reviewed on a regular basis.
- Inbound emails must be scanned by DMARC and acted on.

# 4 DMARC Configuration

Enabling DMARC requires configuration changes in in your domains DNS environment. Configuring DMARC is similar across most platforms, though the exact configuration steps may differ. You must have SPF and DKIM configured prior to setting a DMARC policy. If you have no SPF or DKIM and set DMARC to reject, all messages will fail DMARC checks, which will have a significant impact on email deliverability.

To successfully deploy DMARC You need to:

1. Sign up to a DMARC reporting service.
2. Construct your DMARC policy.
3. Publish the record with p=none in DNS.
4. Test the record.
5. Monitor Email deliverability through your reporting service.
6. Update the policy to p=reject in DNS.
7. Continue to monitor for drops.

It is assumed you have the required access and knowledge to configure the required services.

**Step 1: Sign up to a DMARC reporting service**

Control 15.2.36.C.06 of the NZISM requires Agencies to review DMARC reports on a regular basis. To adhere to this requirement a DMARC reporting tool is required. There are many SaaS DMARC reporting providers. Some are available as part of a Secure Email Management and Administration service in Marketplace [Marketplace | Pae Hokohoko — Infrastructure Managed Services catalogue]

**Step 2: Construct your DMARC record**

When constructing your DMARC record for the domain you need to know:

What policy you are applying to the domain (p=none or p=reject)?
If you're starting out, then p=none ensures mail flows will not be impacted while you review reports.
*NB: There is also a p=quarantine option, which is not recommended. An explanation of this is in the FAQ section.*

- What policy you want applied to any subdomains?
  When DMARC is evaluated on a subdomain and that subdomain has no policy, it will apply the policy of the organisational level domain. Using sp= allows a different policy to be applied to subdomains.
  For example, if a sub-domain like email.marketing.minties.govt.nz does not have a DMARC policy, DMARC will check at the organisational level of minties.govt.nz and will apply that policy. It will not look for a policy at the intermediary level marketing.govt.nz. The sp= entry allows the p= entry to be overridden for subdomains. For example, the minties.govt.nz DMARC record could have p=none then sp=reject. The result is the organisation level domain minties.govt.nz is set to none while all subdomains are set to reject
  *Note: To avoid confusion sp= should only ever be set on organisation level domains.*
- What type of DKIM alignment you require?
  Refer to your DKIM deployment. If you are enforcing strict alignment in DKIM (recommended) then for DMARC adkim=s should be used. If you require relaxed mode use adkim=r

- What type of SPF alignment you require?
  Refer to your SPF deployment. If you are enforcing strict alignment for SPF (recommended) then for DMARC aspf=s should be used. If you require relaxed mode use aspf=r
- Where are your DMARC aggregation (RUA) reports being delivered to?
  Your DMARC reporting service provider will advise the destination address for your DMARC aggregation reports.
  *Note: There is also an option for forensic (RUF) reports. These should not be used due to significant privacy concerns. Refer to the FAQ section for more details.*

DMARC Record construction for the organisation domain minties.govt.nz.

| Policy | Setting |
|---|---|
| Version Tag | V=DMARC1 |
| Domain | minties.govt.nz |
| Record Name | _dmarc.minties.govt.nz |
| Domain Policy | p=reject |
| Subdomain Policy | sp=reject |
| DKIM alignment | adkim=s |
| SPF alignment | aspf=s |
| RUA Report detail | m785336297@dmarcprovider.com |

This will result in the following data record for DNS:

```
v=DMARC1; p=reject; sp=reject; adkim=s; aspf=s; rua=mailto:785336297@dmarcprovider.com
```

**Step 3: Add TXT Records to your DNS**

The following assumes use of the Govt DNS platform, exact steps may vary for other platforms.

Note: Setting a _dmarc record in DNS is enabling DMARC on the domain.

Log in to the DNS portal and browse to your domain.

1. Click on the Current tab under DNS Zones.
2. Click on Edit.
3. Click on the + symbol to add a new row.
4. Set the record name to _dmarc.<your domain>
5. Set the TTL to 3600 (or whatever is required for your domain).
6. Change the type to TXT.
7. Add your record data from the information collected earlier (ref Step 2: Construct your DMARC record).
8. Add a comment or change number if needed for your environment.
9. Click on Publish.
10. Repeat this for other domain records if required.

**Step 4: Test your DMARC Record**

Once DNS records are published, use an external service to check your DMARC record is valid. The DMARC checker on the MXToolbox supertool provides a useful test. (https://mxtoolbox.com/SuperTool.aspx#)

Enter your domain name and select the DMARC Lookup. This will return your record and will show it in a green box if all is good, or a red box if there are errors. If there are any errors it will list them below.

**Step 5: Monitor email deliverability through your reporting service**

After enabling DMARC, monitor email deliverability by regularly reviewing DMARC reports for your domain. The reports will show:

**Sending Sources:**

IP addresses and hostnames of servers sending mail using your domain, which helps identify legitimate senders and unauthorized sources. (e.g. people spoofing your domain)

**Authentication Results:**

Whether SPF and DKIM passed or failed;

Whether they were aligned with the domain in the From: header. (required for DMARC to pass)

**DMARC Disposition:**

What the receiving server did with the message:

- none – Delivered normally
- quarantine – Sent to spam/junk
- reject – Blocked outright

**Message Volume**

Number of messages received from each source, which is useful for spotting sudden spikes or ongoing abuse.

**Policy Evaluation**

Which DMARC policy was applied. (none, quarantine, reject)

Whether the policy came from the domain or a subdomain override.

**Reporting Organization**

The name and contact info of the receiver (e.g., Google, Microsoft) that generated the report.

From this information you should be able to determine if you have any misconfigurations in your SPF or DKIM settings and where any errors are coming from. It is recommended you monitor these reports for a minimum of 4 weeks prior to moving from p=none to p=reject.

If you work with bulk mail sending services you may wish to run test campaigns from your provider to a limited set of recipients to confirm delivery, checking the received email headers for SPF and DKIM, along with checking the DMARC reporting.

**Step 6: Update the DNS _dmarc record to p=reject**

Once your DMARC reports show all expected mail is being delivered correctly, log into the DNS portal and change the p=none and sp=none records to p=reject and sp=reject.
*Note: In theory you do not need the sp setting when the p= and sp= are the same.*

**Step 7: Continue to monitor for drops**

Implement ongoing monitoring of your DMARC records. This should help to identify if there are unauthorised systems trying to impersonate your domains, or highlight any misconfigurations which need addressing. This monitoring is it tends to fairly quickly highlight if someone has implemented a new service, perhaps some shadow IT service, which is trying to send email on behalf of your domain.

## Deploying DMARC on non-mail-enabled domains

The framework requires p=reject policies are applied to all non-mail-enabled domains. This is to aid SPF and DKIM to block as much spoofed mail as possible. As these domains are not involved with email this is a non-impacting setting.

***Example DMARC Record:***

| Name | TTL | Type | Data | Comment |
|---|---|---|---|---|
| _dmarc.<yourdomainname> | 3600 | txt | "V=DMARC1;p=reject; adkim=s; aspf=s; rua=mailto:<your dmarc report RUA email address>" | DMARC reject and report. |

## Configuring DMARC checking on your inbound path

The Framework requires inbound emails are checked for DMARC compliance and acted on based on the sending domains DMARC policy. While most services will do this by default you may need to configure enforcement behaviour. This helps protect your users from incoming non-compliant email.

**Check your email gateway or provider's documentation to confirm whether:**

- DMARC checks are performed on incoming mail,
- The results are logged or exposed, (e.g., in headers or logs)
- Policies (reject, quarantine) are enforced or just reported.

If you're using Microsoft 365, Google Workspace, or an email security service DMARC checks are typically enabled by default. Enforcement behaviour (e.g., whether to reject/quarantine) may need to be explicitly configured.

If you're running your own mail server you'll likely need to install and configure a DMARC verification tool yourself.

**To Ensure DMARC Enforcement is enabled in Microsoft 365:**

Go to Microsoft 365 Defender portal: security.microsoft.com

Navigate to: Email & collaboration → Policies & rules → Threat policies → Anti-phishing

Open the Office365 AntiPhish Default (Default) policy. Scroll to the actions area of the slide out window and look for the following default settings:

- If the message is detected as spoof and DMARC Policy is set as p=quarantine:

  Quarantine the message.

- If the message is detected as spoof and DMARC Policy is set as p=reject:

  Reject the message.

- If the message is detected as spoof-by-spoof intelligence:

  Move the message to the recipients' Junk Email folders.

Settings can be adjusted and custom policies created in line with your Agency’s risk appetite.

# Appendix 1 – DMARC Description

## What is DMARC?

Domain-based Message Authentication, Reporting & Conformance (DMARC) is an email authentication protocol that helps protect your domain from being used in phishing, spoofing, or other fraudulent email activities. It builds on SPF and DKIM by allowing domain owners to publish a policy in DNS that tells receiving mail servers how to handle messages that fail authentication checks. DMARC also provides reporting mechanisms so domain owners can monitor who is sending email on their behalf and how those messages are being handled.

**Here's how DMARC works:**

DMARC works by allowing domain owners to publish a policy in DNS that tells receiving mail servers how to handle messages claiming to come from their domain. When an email is received, the receiving server checks two things:

1. SPF (Sender Policy Framework) – Does the sending IP match the list of authorized senders for the domain, and is the message SPF aligned?
2. DKIM (DomainKeys Identified Mail) – Is the message cryptographically signed by the domain, is the signature valid, and is the message DKIM aligned?

If either SPF or DKIM passes and aligns, the message passes DMARC. If both fail, the receiving server applies the domain's DMARC policy (none, quarantine, or reject) to decide what to do with the message. Meanwhile, the server sends aggregate reports (RUA) back to the domain owner, summarizing authentication results and helping them monitor for abuse or misconfigurations.

**Why DMARC matters:**

DMARC helps to protect your domain from being used in email-based attacks like phishing, spoofing, and business email compromise. Without DMARC, anyone can forge your domain in the "From" address of an email, potentially tricking recipients into trusting malicious messages. DMARC helps prevent this by verifying that emails claiming to come from your domain are actually authorised and authenticated using SPF and/or DKIM. It also gives you visibility into how your domain is being used across the internet through detailed reports, allowing you to detect abuse, misconfigurations, and unauthorised senders — all of which are critical for maintaining email trust.

## DMARC Evaluation logic

DMARC checks two things:

1. Authentication: Did SPF or DKIM pass?
2. Alignment: Did the domain used in SPF or DKIM match the domain in the From: header?

DMARC passes if either SPF or DKIM passes and aligns.

**DMARC Pass / Fail Scenarios**

| SPF Result | SPF Alignment | DKIM Result | DKIM Alignment | DMARC Result |
|---|---|---|---|---|
| Pass | Pass | Fail | Fail | ✅ Pass (SPF aligns) |
| Fail | Fail | Pass | Pass | ✅ Pass (DKIM aligns) |
| Pass | Fail | Pass | Pass | ✅ Pass (DKIM aligns) |
| Pass | Pass | Pass | Fail | ✅ Pass (SPF aligns) |
| Pass | Pass | Pass | Pass | ✅ Pass (both align) |
| Fail | Fail | Fail | Fail | ❌ Fail (neither passes nor aligns) |
| Pass | Fail | Pass | Fail | ❌ Fail (neither aligns) |
| Pass | Fail | Fail | Fail | ❌ Fail (SPF passes but not aligned) |
| Fail | Fail | Pass | Fail | ❌ Fail (DKIM passes but not aligned) |

**What Happens When DMARC Fails?**

The outcome depends on the DMARC policy (p=) set by the domain owner, but may depend on how the recipient configures their inbound policy for handling of DMARC.

| DMARC Policy | Result on Fail | Description |
|---|---|---|
| none | Accept | No enforcement; just monitoring. |
| quarantine | Mark as spam | The email may be delivered as normal, sent to junk/spam folder or silently dropped. |
| reject | Drop | The email is rejected. |

## Adhering to policy for inbound email

As described in Section 4.2 recipient domains can be configured to handle incoming messages using their own settings. This means there is no guarantee of exactly how recipient domains will process received email. As a sender you can have all possible mechanisms in place. If the receiving domain has weak or no DMARC actions in place, spoofed messages can still be delivered.

To protect your userbase it is important you understand DMARC and apply relevant settings, in line with your security posture on your inbound email.

# Appendix 2 – Frequently asked Questions

**Why shouldn't p=quarantine be used?**
P=quarantine has been seen as an interim step between p=none and p=reject. In a business sense this is not good practice because if there is a problem legitimate email may be flagged as spam, sent to junk mail, or silently dropped by the recipient server resulting in inconsistencies. Genuine email being flagged as span or sent to junk mail folders can result in reputational damage.

A better approach is to remain on p=none while monitoring reports and fixing any issues. Once you have identified and validated all legitimate senders from your domain move directly from p=none to p=reject.

**Can I use DMARC Forensic (RUF) Reports?**
No. Do not enable RUF reporting. If you have it enabled, it should be removed from your DMARC record in DNS. The failure options (fo) tag is associated with RUF and also should also be removed if present.
RUF reports often include full message headers, subject lines, and sometimes message bodies, which can contain personally identifiable information (PII) or confidential data. This is a significant privacy concern, as the sender of the email has no knowledge their data may be forwarded outside of the intended destination. In such an instance an RUF report may violate the NZ Privacy Act, especially if the reports sent to third-party processors are stored insecurely.
Major mailbox providers (EG Microsoft and Google) refuse to send RUF reports.

**What happens if a DMARC lookup fails?**
If a DMARC lookup fails at the recipient's end due to an issue like a DNS error, the receiving mail server typically treats the message as if no DMARC policy exists for the domain. Normally this means the message is not subject to DMARC enforcement. The server may still evaluate SPF and DKIM, but DMARC disposition (none, quarantine, reject) is not applied.

**What about DMARCbis or DMARC 2.0?**
DMARCbis is an upcoming revision of the DMARC protocol. It remains in draft and has no exact date for formal publication, though this is generally expected by the end of 2025. It will replace the current DMARC specifications (RFC 7489 and RFC 9091).

DMARCbis (also referred to as DMARC 2.0) is a significant update to the original DMARC protocol. While it retains the same version tag (v=DMARC1) for backward compatibility, it introduces several key improvements aimed at enhancing clarity, security, and operational flexibility.

Formal guidance has not been written by the GCDO for the use of the new DMARCbis tags, however these can be added to your records now. It should be expected the tag np=reject will be added to the framework in future. This instructs DMARC to reject any email coming from a spoofed, non-existent domain.

**What tags should not be used?**
The following tags are not required and should not be used with the deployment of DMARC in line with the Framework:

| Tag | Use | Reason |
|---|---|---|
| ruf | Forensic Reports | Forensic reports create significant privacy concerns. Refer to "Can I use DMARC Forensic (RUF) Reports?" (above) |
| fo | Failure Reporting Options | This is an option used with forensic reporting which is redundant due to not using forensic reporting. |
| pct | Percentage of messages to which the policy applies | This was an old testing methodology used with DMARC applying the policy only to a limited percentage of messages, essentially making DMARC unreliable. It is deprecated in DMARCbis so should not be used. |
| rf | Report Format | This was an option for controlling failure report formats. It is deprecated in DMARCbis so should not be used. |
| ri | Reporting Interval | This was an option for controlling how often aggregated reports were sent. It is deprecated in DMARCbis so should not be used. |

# Appendix 3 – Evaluating DMARC Reporting services

When considering a supplier for DMARC reporting services you should consider the following:

**Report Aggregation & Parsing**

- Automatic collection of aggregate reports from multiple providers.
- Parsing of XML reports into human-readable dashboards.
- Handling of TLS-RPT.

**Visual Dashboards & Analytics showing clear visualisations of:**

- Pass/fail rates for SPF, DKIM, and DMARC.
- Sending sources/IPs and their alignment status.
- Trends over time (daily/weekly/monthly).
- Heatmaps or geolocation maps of sending Ips.
- Filtering by domain, source, result, etc.

**Threat Intelligence**

- Identification of unauthorized senders or spoofing attempts.
- Reputation scoring of sending IPs/domains.
- Integration with threat intelligence feeds.
- Alerts for suspicious activity or policy failures.

**Policy Management & Recommendations**

- Guided policy enforcement. (e.g., from none → quarantine → reject)
- Simulations or “what-if” analysis before changing policy.
- SPF/DKIM alignment checks and misconfiguration warnings.

**Multi-Domain & Subdomain Support**

- Centralized management of multiple domains.
- Separate or inherited policies for subdomains.
- Delegation of access to different teams or business units.

**Automation & Integrations**

- Automated DNS record generation for DMARC, SPF, DKIM.
- API access for integration with SIEMs or internal dashboards.
- Email alerts or webhook notifications for failures or anomalies.

**Data Retention & Export**

- Long-term data retention. (e.g., 6–12 months or more)
- Ability to export reports. (CSV, JSON, PDF)
- Audit logs for compliance tracking.

**Security & Compliance**

- Data encryption at rest and in transit.
- Compliance with ISO 27001, or other relevant standards.

- Role-based access control. (RBAC)

**Support & Documentation**

- Responsive support team.
- Detailed documentation and onboarding help.
- Training resources or customer success managers.

# Appendix 4 – List of Acronyms

| Acronym | Definition |
|---|---|
| adkim | Alignment for DKIM |
| aspf | Alignment for SPF |
| CNAME | Canonical Name (used as an alias in DNS) |
| DKIM | Domain Keys Identified Mail |
| DMARC | Domain-based Message Authentication, Reporting, and Conformance |
| DNS | Domain Name System |
| ESP | Email Service Providers (Typically referring to bulk senders) |
| M365 | Microsoft 365 |
| MX | Mail Exchange |
| NZISM | New Zealand Information Services Manual |
| p | Policy |
| r | Relaxed (for policy tag) |
| rua | Reporting URI for Aggregate reports |
| ruf | Reporting URI for Forensic reports |
| s | Strict (for policy tag) |
| SaaS | Software as a Service |
| SGE | Secure Government Email (Framework) |
| sp | Subdomain Policy |
| SPF | Sender Policy Framework |