# September 2022 New Zealand Information Security Manual v3.6 Release

**Change Area: Public Cloud Security (New Chapter)**

**Rationale:**

In July 2016, Cabinet agreed that agencies can also use public cloud to deliver office productivity services, provided they comply with security guidance issued by the GCDO and the GCSB, but the NZISM has not provided any detailed guidance on this.

**Change Description:**

A new chapter has been written which will provide information security guidance on key security concepts and architecture patterns related to public cloud services.

Topics included in this chapter cover: An introduction to Public Cloud Security Concepts; Governance, Risk and Assurance; Identity Management and Access control; Data Protection; Logging and Alerting.

**Expected Outcome:**

Agencies understand key concepts and implement controls related to securing their use of public cloud services.

**Change Area: Inverse Split-Tunnel VPN (New Section)**

**Rationale:**

Architecture advice advocates for the use of inverse split tunnelling, where an explicit list of authorised and trusted internet based services are able to be directly accessed, bypassing agency perimeter controls.  Both the architecture advice, and the NZISM, advise against the use of full split tunnelling.

**Change Description:**

A new section on Inverse Split tunnelling has been written for Chapter 18 Network Security. This section covers information relating specifically to configuring secure remote access services (also known as VPN services) for agency devices that facilitate agency information (e.g. documents or emails) being transferred to remote systems.

**Expected Outcome:**

Agencies identify and effectively manage the risks and compensating controls involved in utilising inverse split tunnelling as part of remote access virtual private network (VPN) configurations.

**Change Area: Language Modernisation (Whole NZISM)**

**Rationale:**

A survey of international national cybersecurity centres, standards associations, professional associations, and private companies shows broad consensus to update terminology. A current NZ survey shows the NZ public does not accept language which perpetuates racism.

**Change Description:**

There are a number of computing terms that should be avoided in professional writing, since they are not strictly needed and are considered offensive or exclusionary by some groups. In this release whitelist, blacklist, and man-in-the-middle have been updated; other terms will be updated in future releases.

**Expected Outcome:**

The NCSC encourages New Zealand organisations to adopt and normalise these new terms.

**Change Area: DMARC (Domain-based Message Authentication, Reporting and Conformance); DKIM (DomainKeys Identified Mail) (Update to section 15.2)**

**Rationale:**

Phishing and malware distribution attacks are common internet security threats. To limit the possibility of agency domains being used fraudulently (e.g. for spam or spear-phishing), agencies should implement: a Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM); and Domain-based Message Authentication, Reporting & Conformance (DMARC) records.

Agencies have had some time to start implementing the full provisions of DMARC/DKIM and it was always the intention of the NZISM to change these to MUST controls. The future replacement for SEEMail will use DMARC and therefore vendors and agencies will need to be compliant.

**Change Description:**

1. Change of DMARC control compliance from SHOULD to MUST [CID:6019] [CID:6021]

2. Change of DMARC policy setting from p=”none” to p=”reject” [CID:6020]

3. Change of DKIM control compliance from SHOULD to MUST [CID:1797] [CID:1798]

**Expected Outcome:**

A reduction in the number of Government email domains being used for spam or email phishing campaigns.