



Cyber Security Action Plan 2026–2027

Our vision: A New Zealand that embraces cyber security to enable innovation, drive a prosperous economy and protect our digital way of life



UNDERSTAND

We – government, organisations, and individuals – are well aware of cyber risks and know how to protect ourselves



PREVENT AND PREPARE

We manage cyber risks to prevent harm and be well prepared for incidents when they occur



RESPOND

We react effectively and decisively to adverse cyber incidents



PARTNER

Our resilience to cyber threats is bolstered by strategic and targeted cooperation

IMMEDIATE ACTIONS TO IMPROVE CYBER SECURITY

ACTIONS

1. Establish a single point for cyber incident reporting to improve quality of data and make it easier to access advice, guidance and help in response and recovery from cyber incidents.

LEAD AGENCY: **NCSC**

2. Provide critical infrastructure operators with practical guidance and support to strengthen cyber resilience.

LEAD AGENCY: **NCSC**

3. Increase responsiveness to the national security risks of emerging technologies.

LEAD AGENCY: **DPMC**

ACTIONS

4. Develop options to improve the cyber security of critical infrastructure, including through public consultation on regulatory proposals.

LEAD AGENCY: **DPMC**

5. Strengthen the mandate of the Government Chief Digital Officer to ensure government digital products and services are secure and resilient.

LEAD AGENCY: **GCDO**

6. Ensure higher and more consistent security standards are embedded in digital procurement and design across government and reduce duplication among government agencies.

LEAD AGENCY: **NCSC**

7. Enable New Zealand to process and manage quantum-resistant cryptographic material to ensure our most sensitive information is protected against evolving cyber threats.

LEAD AGENCY: **NCSC**

8. Provide advice on options to incentivise the protection of personal information from cyber threats, such as introducing a civil pecuniary penalty regime to the Privacy Act 2020.

LEAD AGENCY: **MOJ**

ACTIONS

9. Manage public service use of high-risk vendors, services and products to reduce risks to government-held data.

LEAD AGENCIES: **DPMC + PSC**

10. Update legislative powers to enable New Zealand’s security sector agencies to use cyber capabilities and tools to advance our national security interests.

LEAD AGENCY: **DPMC**

11. Provide advice on a potential new offence targeted at people who view, possess, or disseminate personal information when they are aware it has been illegally obtained.

LEAD AGENCY: **MOJ**

ACTIONS

12. Work with partners to maintain lawful access while also protecting personal data, privacy and cyber security.

LEAD AGENCY: **DPMC**

13. Expand and deepen the NCSC’s collaboration with cyber security industry partners to prevent, detect and respond to malicious cyber activity.

LEAD AGENCY: **NCSC**

14. Bolster cyber resilience in the Pacific and strategically engage on regional digital and technology issues.

LEAD AGENCIES: **MFAT + NCSC**

15. Support the international rules and norms related to responsible state behaviour in cyberspace.

LEAD AGENCIES: **MFAT + DPMC**

This Action Plan sets out key initiatives that the New Zealand Government will deliver over the next two years. It does not represent all current or planned activities to protect New Zealanders from cyber harm and uplift our cyber security. Adapting to changes in the threat environment and new technologies means the Action Plan will be reviewed regularly and actions updated, added or removed as required to remain current and relevant.