COOK ISLANDS CYBER SECURITY POLICY 2024

Protecting the Cook Islands against cyber security threats, now and into the future

What is cyber security?

Cyber security is about protecting Cook Islanders.

It protects our people's personal information, our country's reputation, our Government's sensitive information, the infrastructure we rely on, our businesses, and our connections to the world.

All information in the Cook Islands, including that online, has value and should be protected.

We are basing our cyber security policy in ka'a

The policy draws on research methodology of the NSDA ka'a, the braided sennit cord of the coconut. Braiding and knotting the ka'a require a careful selection of coconut husks and strands.

- Our policy must be braided into existing Cook Island policies, including the NSDA.
- Our policy's fibres will be woven with knowledge, wisdom and guidance provided by Cook Islanders.

PILLAR 1 ONLINE HARM AND CYBERCRIME

Our people feel safe.

Communities feel safe online. They know where to go for advice and support on cyber harm.

- Improve cybersecurity and cybercrime legislation. (NSP PAF 8.2)
- Upgrade law enforcement agencies' digital crime detection systems, including those relating to objectionable content. (NSP PAF 8.2)
- Establish a Cook Islands Computer Emergency Response Team. (NSP PAF 8.4)
- Explore opportunities for gaining access to additional support from international partners for addressing cybercrime. (NSP PAF 8.5)
- Explore opportunities to become a party to the Budapest Convention on Cybercrime and other treaties. (NSP PAF 8.5)

PILLAR 2 OUR GOVERNMENT

Our government is strong.

Government defences are strengthened to keep our most sensitive information safe and secure.

- Develop guidelines for assessing cyber security risks in Government procurement and acquisition of technology and hardware.
- Enable Government-wide purchasing decisions on secure and resilience technology.
- Integrate assessment of cyber security risks into security and disaster planning.
- Develop a cyber security emergency response plan.
- Establish methods for reporting and data collection on cyber security risks and incidents within Government.
- Advocate for increased caucusing on regional cyber issues.
- Explore the use of the National Security Committee to take strategic decisions on cyber issues.
- Protect access to our security related information through the protective security requirements framework. (NSP PAF 1.6)
- Develop a cybersecurity prevention plan leveraging support of regional partnerships, such as the Cyber Safety Pacifica program and Get Safe Online Cook Islands.

PILLAR 3 OUR PEOPLE

We're all cyber warriors.

We're empowered to protect ourselves online. We retain cyber professionals in the Cook Islands and train people up.

- Build on existing cybercrime prevention initiatives through strengthening awareness campaigns to upskill communities, including Cook Islands cyber security stories.
- Establish strong regional and international connections so we can access expertise when required.
- Encourage cyber security tertiary qualifications and establish study and career pathways in cyber. (National ICT Policy 9.3.4)
- Upskill our Government workers through secondments and training for Government staff, including partnering with the New Zealand Government in the first instance.
- Develop interventions to encourage retention of ICT professionals. (National ICT Policy 9.3.4)

PILLAR 4 CRITICAL NATIONAL INFRASTRUCTURE

Our infrastructure is protected.

Our most important infrastructure is protected from cyber harm.

- Develop guidelines and tools for assessing cyber security risks in critical infrastructure.
- Conduct a comprehensive cyber risk assessment for the port, airport, and other critical infrastructure to proactively reveal cyber gaps and issues.
- Consider minimum standards and guidelines for critical infrastructure providers (such as reporting criteria for cyber security incidents).
- Include cyber resilience requirements in service-level agreements with critical infrastructure providers and their key suppliers.
- Assess risks, benefits, and mitigations of offshore data storage and control of automated systems.

How we will deliver our policy

In the first two years of this policy, we will focus on areas where rapid action is required to address critical risks or enable further work.

- Implement the *Cyber Investment Plan Roadmap.* (Enables this cyber security policy)
- Improve cyber security and cybercrime legislation. (NSP PAF 8.2)
- Establish a national cyber emergency response team (CERT) for implementation in 2025–2026. (NSP PAF 8.2)
- Explore opportunities for gaining access to additional support from international partners for addressing cybercrime. (NSP PAF 8.5)
- Develop a cyber security emergency response plan.

RELEVANT POLICIES

National security policies and strategies are available at pmoffice.gov.ck

National Security Policy Performance Assessment Framework (NSP PAF)

National Information Communications Technology (ICT) Policy

Te ara akapapa'anga nui –national sustainable development agenda (NSDA)