Sense of Security

MAKING SENSE OF

NSW GOVERNMENT

NSW Government Cyber Security Policy

The mandatory requirements that all agencies must implement along with strategies to mitigate cyber risk.

NSW Cyber Security Policy came into effect from February 2019. The new Cyber Security Policy replaces the NSW Digital Information Security Policy 2015 and is an outcome of the NSW's cyber security strategy.

As part of the reporting obligations, a report on cyber security maturity needs to be submitted to agency head and GCISO by August 31st each year.

What are the requirements?

The mandatory requirements are:

- Planning and Governance
- Cyber Security Culture / Awareness
- Manage Cyber Security Risks
- Resilience against cyber attack
- Report against the requirements

Planning and Governance

Ensure that a governance committee is in place to be accountable for cyber security policies, risk and compliance.

Cyber Security Risk Assessments are conducted as part of the agencies overall risk assessment process.

Agencies must be accountable for the cyber security risk for IT service providers and other third party providers.

Cyber Security Culture / Awareness

- Increase cyber security awareness/training to all staff. This should also include simulation exercises.
- Access to sensitive information or systems. Privilege systems must be tightly controlled to ensure they are accessed on a needs basis. This may include removing access to systems for staff who do not require access or who's employment is terminated.

Manage Cyber Security Risk

- Implement an Information Security Management System (ISMS)
- Implement and report on the maturity against ACSC Essential 8
- Information classification based on criticality. Identify the organisations critical systems or 'crown jewels'.
- Security must be baked into the system development life-cycle (SDLC) including agile projects
- Trials and activity logging to ensure integrity of data.

Resilience against cyber attack

Cyber incident response plan that integrates with the agency incident management process.

Cyber incident response plan testing every year with business stakeholders such as IT executives, media and communication teams.

Report the requirements

Annual Report must be submitted by August 31 to GCISO and agency head which must include:

- Cyber Security risk with residual rating.
- Crown jewels identified
- Attestation on cyber security

How can SOS help?

Sense of Security's Governance, Risk and Compliance Practice employs experienced ISO 27001 Lead Auditors and Implementors that can assist any organisation develop and implement an effective security strategy that aligns to the latest NSW Cyber Security Policy.

SOS's roadmap strategy to achieve compliance to NSW Cyber Security Policy is as follows:

LEAD

Security forum and governance structure

Cyber Security Risk Assessment and remediation plan

ISMS Framework

Roles and Responsibilities

PREPARE

Cyber Security Awareness Program

Review Access Control to sensitive information

Support in communicating security threat to other agencies to manage cyber-risk

PREVENT

Maturity assessment based on ACSC Essential 8

Document policies, standards and processes

Risk Treatment: This may include Vulnerability management Program, SDLC, Fraud detection

System Classification and identification of 'Crown Jewels'

DETECT, RESPOND & RECOVER

Develop Cyber Security Incident Plan

Annual Cyber Security Incident Plan testing

Deploy monitoring process for identification of incidents

REPORT

Assist in preparing Annual Report by August 31 to GCISO and agency head that includes:

- Cyber Security risk with residual rating.
- Crown jewels identified
- Attestation on cyber security

Sense of Security

Contact us to discuss how our security solutions can help protect your most vital assets

1300 922 923 or +61 (2) 9290 4444
info@senseofsecurity.com.au
senseofsecurity.com.au