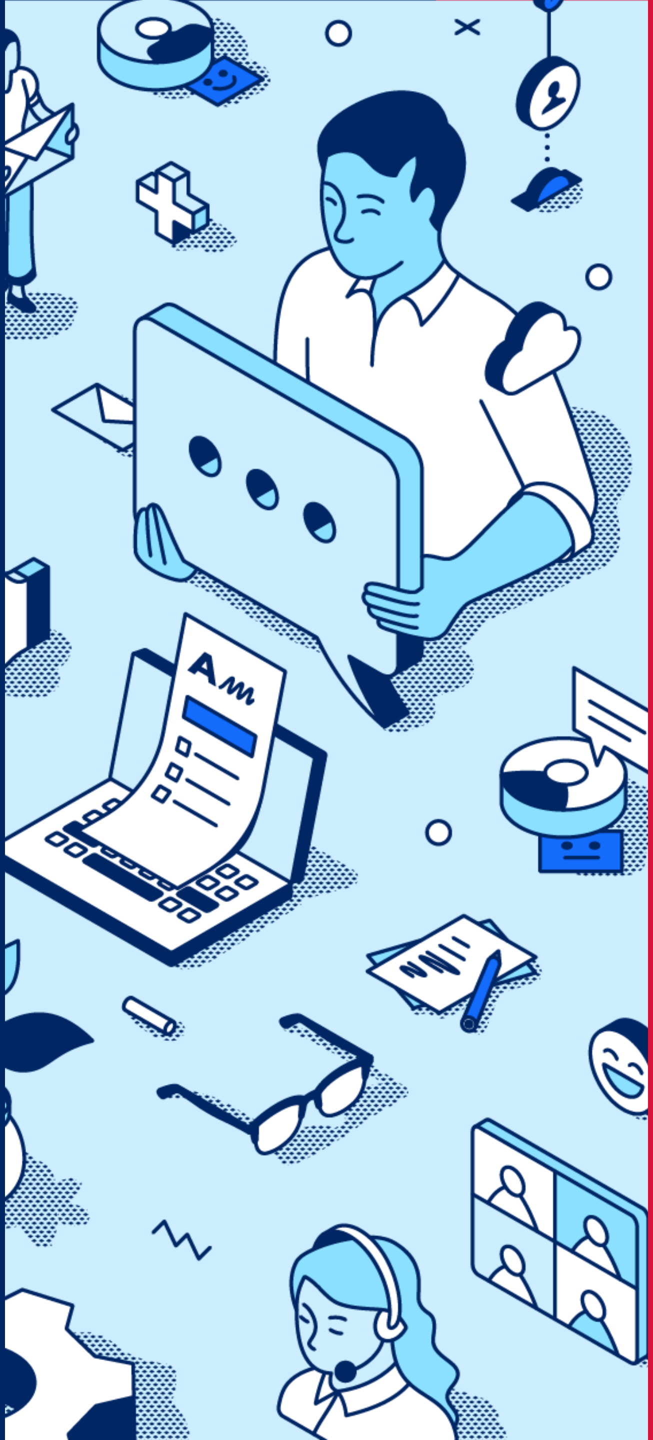
Cyber Security NSW

Cyber Security for Local Government

2024 Statewide Mutual
Risk Management Conference

Jack Boyd – Awareness, Development & Resilience
Sharon Lee – Intelligence & Incident Response

August 2024



NSW
GOVERNMENT

Acknowledgment of Country

What we'll cover…

01 Introduction and Cyber Security NSW overview

02 NSW Government and councils cyber threat landscape

03 Cyber Risk and Governance – NSW vs local government

04 Cyber Security NSW services for local government

1

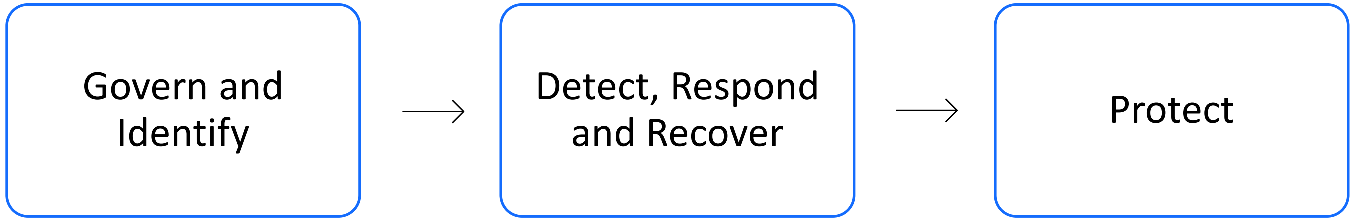
Cyber Security NSW Overview

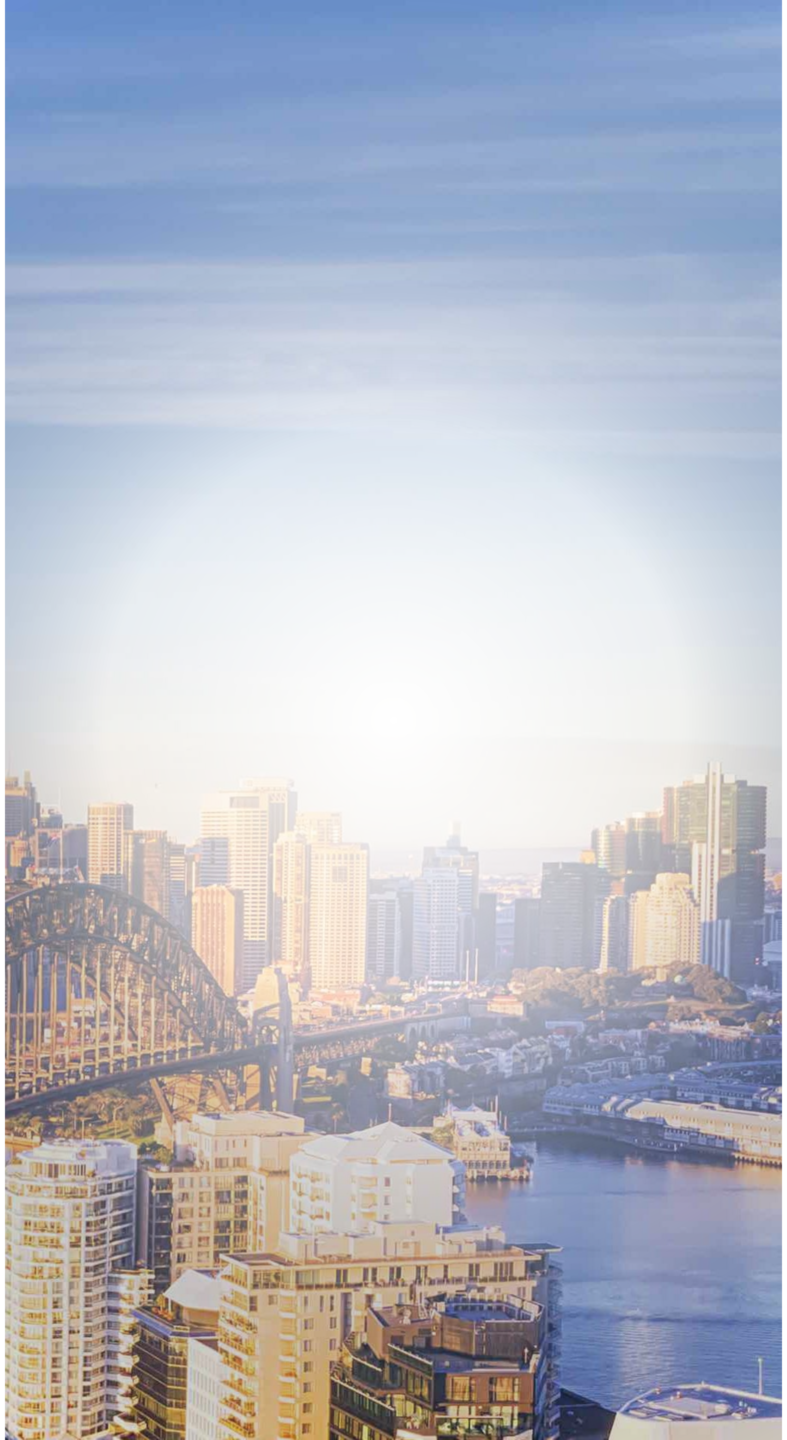
Cyber Security NSW

Our role

To achieve a cyber-secure NSW Government, Cyber Security NSW:

- ✓ **delivers** products, services and best practice advice and guidance to NSW Government departments, agencies and councils
- ✓ **coordinates** all-of-government cyber security strategies
- ✓ **leads** the NSW Government response to significant cyber security incidents and cyber crises


Govern and Identify → Detect, Respond and Recover → Protect



What we provide

Best practice advice and guidance

Security assessments

Incident response

Leadership and coordination

Awareness and training

Threat intelligence

NSW Cyber Security Policy

What is cyber security?

The measures used to protect systems from compromise of confidentiality, integrity and availability

- ✓ Technology
- ✓ People
- ✓ Process

Cyber security requires a layered approach

Importance of cyber security

In FY23, there were 150 data breaches, **up 85% from previous FY**

Self-reported losses due to BEC in Australia was almost **$80 million**

Social engineering was again a contributing factor **in over ½ of confirmed cases in NSW**

Cyber Security NSW

2023 NSW Government Cyber Threat Report

September 2023

Australian Government
Australian Signals Directorate

ASD Australian Signals Directorate
ACSC

ASD Cyber Threat Report

2022–2023

2

Cyber Threat Landscape

2023 NSW Government Cyber Threat Report

74% of reported data breaches were of organisations with no direct link to the NSW Government – the common element was staff misusing their work email for personal reasons.

Publicly accessible remote management interfaces have emerged as one of the most common attack vectors.

Cybercriminal groups have been highly effective at exploiting **vulnerabilities in managed file transfer software.**

Reports of **subdomain takeovers and hijacking of websites and social media accounts managed by NSW Government** entities have been increasing.

The number of internal actors identified – where **internal users caused or contributed to an incident** – almost tripled.

Public claims of cyber attacks by threat actors against entities **should be investigated immediately** to determine legitimacy or cases of misattribution.

It is likely **ransomware operators** will continue to conduct data extortion – though stolen data may also be used for further malicious activity or sold to other threat actors for profit.

91% of ransomware incidents were the result of a third-party's environment being breached rather than a direct attack on NSW Government systems and networks.

Stolen credentials and the **installation of unauthorised software** were the most common tactics used to compromise environments

Sensitive and non-sensitive information can be aggregated by threat actors to enable the identification of targets and individuals.

Note: Analysis is from reported cyber incidents only across FY22/23

2023 Local Government Cyber Threat Report

Top five actions observed in successful attacks

- Phishing
- Maintenance error
- Misconfiguration
- Influence
- Email misuse

Threat actors continue to employ phishing and other social engineering techniques when targeting the NSW Government, with phishing attempts successful in the majority of reported incidents.

Source: Cyber Security NSW Annual Threat Report 2023

Cyber threat actor types

External threat actors:

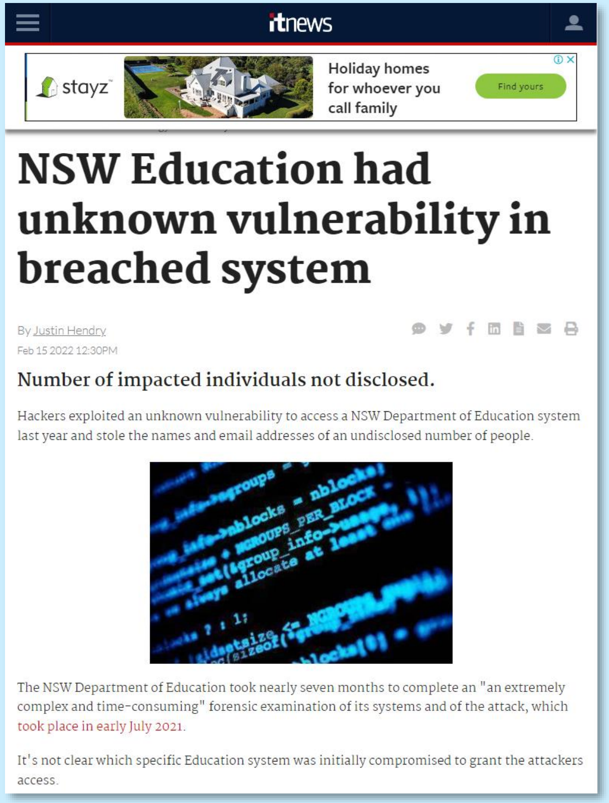
- Criminals – financial gain
- Hacktivists – ideology and issues motivations
- Nation states and their proxies – political, social and economic progress in their national interest

Internal

- Staff or contractors – sabotage, trusted with potential escalated privileges

Partner

- Third parties such as managed service providers, vendors, suppliers – information shared or stored



NSW Education had unknown vulnerability in breached system

By Justin Hendry
Feb 15 2022 12:30PM

Number of impacted individuals not disclosed.

Hackers exploited an unknown vulnerability to access a NSW Department of Education system last year and stole the names and email addresses of an undisclosed number of people.

The NSW Department of Education took nearly seven months to complete an "an extremely complex and time-consuming" forensic examination of its systems and of the attack, which took place in early July 2021.

It's not clear which specific Education system was initially compromised to grant the attackers access.

What are we protecting?

Information, business systems, IT infrastructure, critical infrastructtre and council services are regarded as assets that require protection

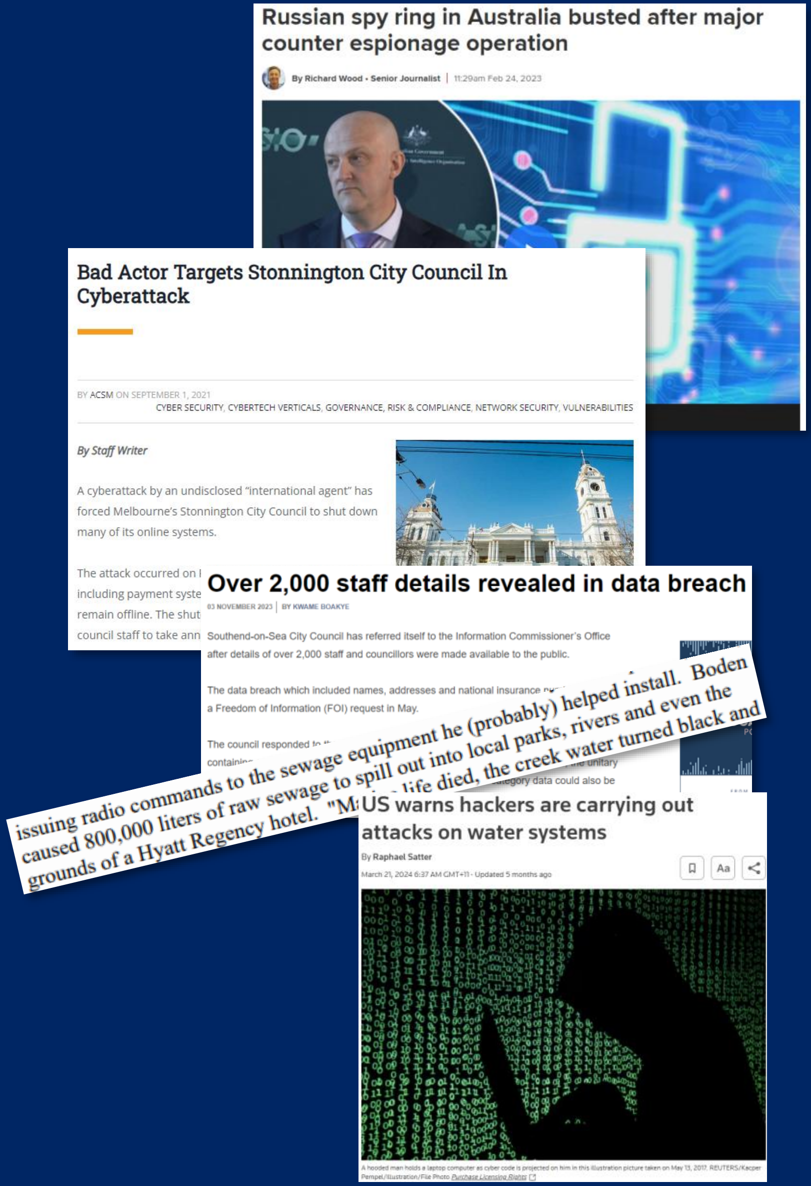
Protecting them protects individuals and the local economy and contributes to national security

To protect assets, we need to understand which are most sensitive, valuable and vulnerable to attack

We look at supporting technologies, processes and dependencies to understand the current state

Protecting from what?

- Once we understand assets, intelligence collection and assessment highlight the threats we might face
- ‘Cyber’ isn’t a threat. Criminals, nation-states and their proxies and issue-motivated individuals or groups are threats
- Malicious actors have motivations, which help us assess their relevance
- Threats can be non-malicious, such as emailing the wrong person



Russian spy ring in Australia busted after major counter espionage operation

By Richard Wood • Senior Journalist | 11:29am Feb 24, 2023

Bad Actor Targets Stonnington City Council In Cyberattack

BY ACSM ON SEPTEMBER 1, 2021
CYBER SECURITY, CYBERTECH VERTICALS, GOVERNANCE, RISK & COMPLIANCE, NETWORK SECURITY, VULNERABILITIES

By Staff Writer

A cyberattack by an undisclosed “international agent” has forced Melbourne’s Stonnington City Council to shut down many of its online systems.

The attack occurred on
including payment syste
remain offline. The shut
council staff to take ann

Over 2,000 staff details revealed in data breach

03 NOVEMBER 2023 | BY KWAME BOAKYE

Southend-on-Sea City Council has referred itself to the Information Commissioner’s Office after details of over 2,000 staff and councillors were made available to the public.

The data breach which included names, addresses and national insurance
a Freedom of Information (FOI) request in May.

The council responded
containing
the unitary
category data could also be

issuing radio commands to the sewage equipment he (probably) helped install. Boden
caused 800,000 liters of raw sewage to spill out into local parks, rivers and even the
grounds of a Hyatt Regency hotel. "M life died, the creek water turned black and

US warns hackers are carrying out attacks on water systems

By Raphael Satter

March 21, 2024 6:37 AM GMT+11 · Updated 5 months ago

A hooded man holds a laptop computer as cyber code is projected on him in this illustration picture taken on May 13, 2017. REUTERS/Kacper Pempel/Illustration/File Photo *Purchase Licensing Rights*

Is local government a target?

Foreign threat actors do not distinguish between federal, state and local government

Any organisation that provides value is a target

Governments are an opportunity for reputation damage and widespread service disruption

Local government provides essential services and protects critical infrastructure

There are many examples from within NSW

LockBit 3.0 Ransomware Group

ASD ACSC

Countering the insider threat

A security manager's guide

ASIO

2023 NSW Government Cyber Threat Report

September 2023

CyberCX

Ransomware and Cyber Extortion

How to protect your organisation

Weekly Report

CSWR-23046

CrowdStrike Intelligence Weekly Report

Week of 11 November 2023

CROWDSTRIKE GLOBAL INTELLIGENCE TEAM

CROWDSTRIKE

Threat Intelligence

- Helps narrow the scope of security defence activities
- Intelligence reduces fear and uncertainty and supports clear thinking and decision-making
- Creates a proactive security culture
- Focuses on what is real and dangerous – eliminates noise
- Allows specific controls to be implemented and measured
- It isn’t just about ‘cyber’ and isn’t just technical –includes insider threats, events, accidents and natural disasters
- Is available from internal, public, government and commercial sources

3

Cyber Risk and Governance

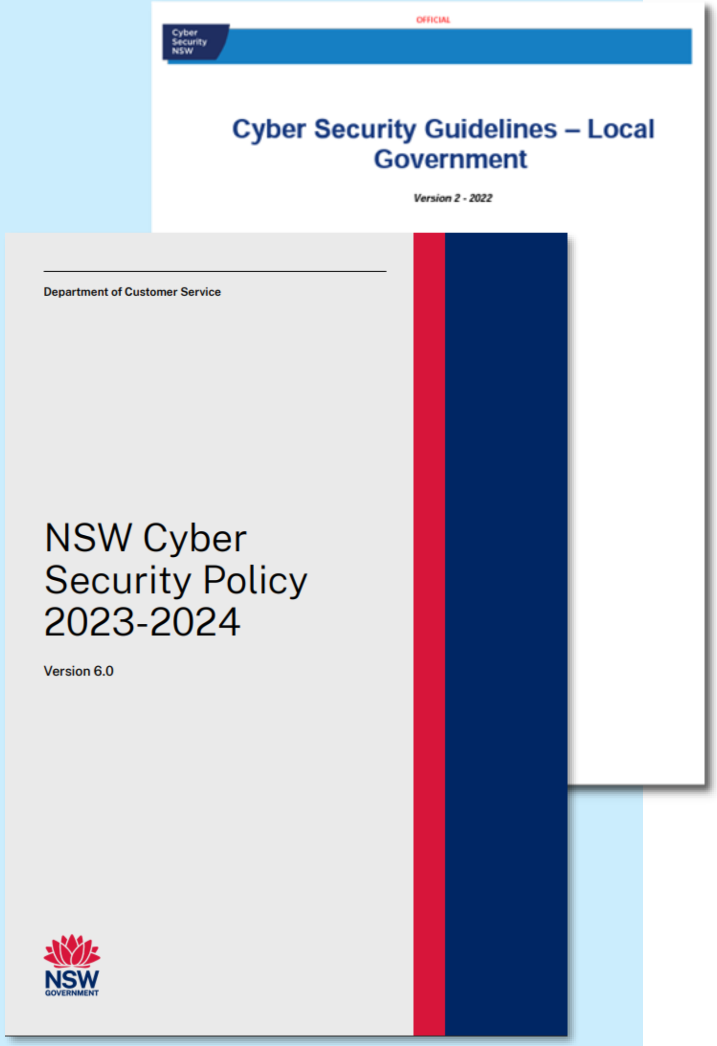
NSW Cyber Security Policy and Guidelines

31 mandatory requirements and responsibilities to manage cyber security risks

✓ All agencies must comply with the **NSW Cyber Security Policy**

✓ Councils are encouraged to adhere to the **Cyber Security Guidelines - Local Government**

The Policy is intended as the initial step rather than the culmination of your cyber security measures



OFFICIAL

Cyber Security NSW

Cyber Security Guidelines – Local Government

Version 2 - 2022

Department of Customer Service

NSW Cyber Security Policy 2023-2024

Version 6.0

NSW GOVERNMENT

Cyber Security Guidelines for Councils

Based on the NSW Cyber Security Policy

Govern & Identify

Implement planning and governance to support asset management and risk minimisation.

Detect, Respond & Recover

Uplift organisational resilience to rapidly detect, respond and recover from cyber incidents.

Protect

Safeguard the organisation by implementing technical controls and conducting awareness activities.

Our policy can be directly accessed here:
https://www.digital.nsw.gov.au/sites/default/files/2024-02/NSW-Cyber-Security-Policy-2023-2024.pdf

31 Mandatory Requirements

Outlined below are the 31 mandatory requirements per the NSW Cyber Security Policy 2023-2024

Govern & Identify

1.1 Allocate and perform roles and responsibilities for cyber security.

1.2 Have an executive-level governance committee with appropriate authority to make decisions about cyber security, including OT/IoT.

1.3 Ensure that the Audit and Risk Committee (ARC) is briefed regularly on cyber security risks, related issues and corrective actions.

1.4 Develop and maintain a cyber security strategy.

1.5 Develop and maintain formalised plans, policies and processes for cyber security practices.

1.6 Establish and maintain processes for asset inventory management and identify asset dependencies.

1.7 Assess and identify Crown Jewels and classify systems.

1.8 Govern the identification, retention and secure disposal of data.

1.9 Define risk tolerance and risk appetite and manage cyber security risks.

1.10 Identify and manage third-party service provider risks, including shared ICT services supplied by other NSW Government agencies.

1.11 Establish and maintain vulnerability management processes.

1.12 Ensure cyber security requirements and impacts are assessed as part of change management processes.

Detect, Respond & Recover

2.1 Implement event logging and continuous monitoring to detect anomalous activity.

2.2 Maintain a cyber incident response plan and use exercises and post-incident reviews to continuously improve the plan.

2.3 Report cyber incidents and provide information on threats to Cyber Security NSW.

2.4 Include cyber security in business continuity and disaster recovery planning.

Protect

3.1 Conduct awareness activities, including mandatory cyber security awareness training.

3.2 Implement access controls to ensure only authorised access.

3.3 Patch applications (ACSC Essential Eight).

3.4 Patch operating systems (ACSC Essential Eight).

3.5 Implement multi-factor authentication (ACSC Essential Eight).

3.6 Restrict administrative privileges (ACSC Essential Eight).

3.7 Implement application control (ACSC Essential Eight).

3.8 Securely configure Microsoft Office macro settings (ACSC Essential Eight).

3.9 Implement user application hardening (ACSC Essential Eight).

3.10 Maintain backups of important data, software and configuration settings (ACSC Essential Eight).

3.11 Establish and maintain secure configurations.

3.12 Define and implement data security controls.

3.13 Implement email security controls.

3.14 Implement controls for endpoint protection, including mobile devices.

3.15 Implement network security controls.

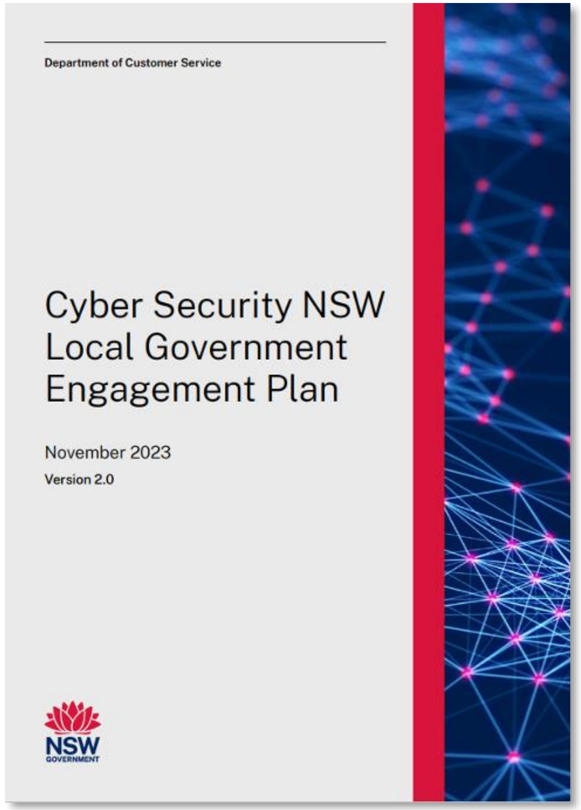
Local Government Engagement Plan

Purpose and Scope

- The Cyber Security NSW Local Government Engagement Plan outlines the model for engagement between NSW local government entities and Cyber Security NSW.

- Engagement encompasses the delivery of a wide range of tailored products, services and best practice advice and guidance to NSW local government entities.

- The Plan outlines streams of engagement, expectations of local government entities, a prioritisation strategy and challenges to consider when seeking assistance.



Department of Customer Service

Cyber Security NSW
Local Government
Engagement Plan

November 2023
Version 2.0

Local Government Engagement Plan

Principles of Engagement

Purposeful

Cyber Security NSW will focus on clearly defined objectives from initiation of each engagement. Meaningful engagement will rely on knowledge of who we need to engage with, an understanding of the outcomes to be achieved, and which activities will be most effective to reach those outcomes.

Timely

NSW local government entities will be informed of how and when they will be involved. Our engagement process will be clearly explained with the inclusion of proposed timelines and schedules.

Inclusive

Engagement will be undertaken in a way that enables all NSW local government entities to participate, regardless of factors such as size, location and cyber security maturity. A flexible approach to engagement ensures the inclusion of all NSW local government entities.

Transparent

Engagement with NSW local government entities will be open and honest. Our engagement process will be clearly explained, as will the role of NSW local government entities and how their input will inform the project. Clear expectations will be set and communicated from the outset of engagement.

Respectful

Cyber Security NSW acknowledges and respects the expertise, perspective and needs of NSW local government entities. We will engage in a way that is open to alternative views and ideas. Our communication will be adapted to meet the needs and preferences of NSW local government entities wherever possible.

Tailored

Cyber Security NSW acknowledges that each NSW local government entity has its own unique environment and circumstances. Through consultation, our approach will be tailored to enable the most efficient and productive service offerings for each NSW local government entity.

Prioritised

A needs-based prioritisation process will be used to ensure engagement with NSW local government entities is effective. Engagement with NSW local government entities is prioritised to ensure outcomes are realistic, achievable and supported throughout the engagement.

Local Government Engagement Plan

Levels of Engagement

Inform	Consult	Involve	Collaborate
One-way communication to inform and educate the NSW local government entity.	Information and feedback sought from the NSW local government entity.	Cyber Security NSW works directly with the NSW local government entity through two-way communication, ensuring the entity's issues and concerns are considered and understood.	Cyber Security NSW will work in partnership with the NSW local government entity to develop mutually agreeable solutions and a joint plan of action.
• Information disseminations • Presentations	• Surveys • Meetings	• Forums • Workshops • Inclusive decision-making processes	• Joint projects • Multi-council initiatives and partnerships

Local Government Engagement Plan

Streams of Engagement

Readily Available

These services are readily available to all NSW local government entities:

- live cyber security awareness training
- cyber security awareness training e-modules
- adaptable training deck for in-house use
- access to an external learning platform
- awareness campaigns and materials
- templates and resources
- NSW Cyber Security Policy guidance
- Local Government – Cyber Security Guidelines
- whole-of-government advice
- best practice advice and guidance
- domain-based message authentication, reporting and conformance (DMARC) support
- threat assessments
- intelligence products (alerts, advisories, briefs and reports)
- vulnerability identification and
- remediation products
- CoP and other forums, including the Local Councils Forum.

Local Government Engagement Plan

Streams of Engagement

Incidents

The incident stream is targeted at local government entities that are having or have had a cyber security incident. The following services focus on incident response and are provided as required:

- ✓ incident triage and containment, including assistance, coordination and advice
- ✓ digital forensics
- ✓ team augmentation, such as providing resources for a dedicated amount of time to support security operations activities
- ✓ dark web monitoring.

Local Government Engagement Plan

Streams of Engagement

Risk and Resilience

The maturity stream focuses on the long-term uplift of cyber resilience and risk management. It may be utilised either on the request of a local government entity or approach by Cyber Security NSW when an entity is identified as requiring assistance. Maturity services and products include:

- passive and intrusive external scanning
- internal vulnerability scanning
- penetration testing
- Essential Eight (E8) Health Checks
- password hygiene assessments
- key website monitoring
- open-source intelligence (OSINT)
- access to a vulnerability risk management platform
- assessment of vendor security risk
- ACSC vulnerability data, e.g. CHIPs and HOTCHIPs
- exercise-as-a-service (EaaS)
- policy advice
- strategic cyber security assurance
- strategic cyber security contract advice.

Local Government Engagement Plan

Streams of Engagement

Executive

The executive stream focuses on improving the awareness and buy-in of the executive teams of local government entities. Executive services include:

✓ proactive engagement by Cyber Security NSW with local government executives, including through the Audit Risk and Improvement Committee

✓ guidance on how to promote awareness of cyber security issues within local councils and other local government entities.

Local Government Engagement Plan

Benefits of working with Cyber Security NSW

✓ Effective governance controls

- Enhanced trust in government
- Strong cyber security foundation
- Effective, risk-based strategy

✓ Reduced likelihood of compromise

- Improved cyber risk management
- Cyber-aware workforce
- Preventing cost of recovery

✓ Proactive detection

- Vulnerabilities identified across assets
- Prioritisation of remediation actions
- Mitigation to prevent exploitation

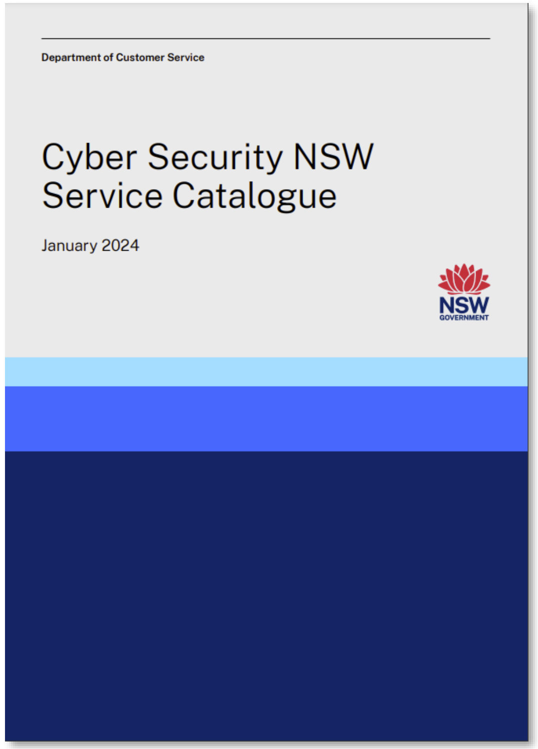
✓ Rapid response

- 24/7 support when incidents occur
- Expert advice and technical support
- Efficient and speedy remediation

4

Cyber Security NSW services

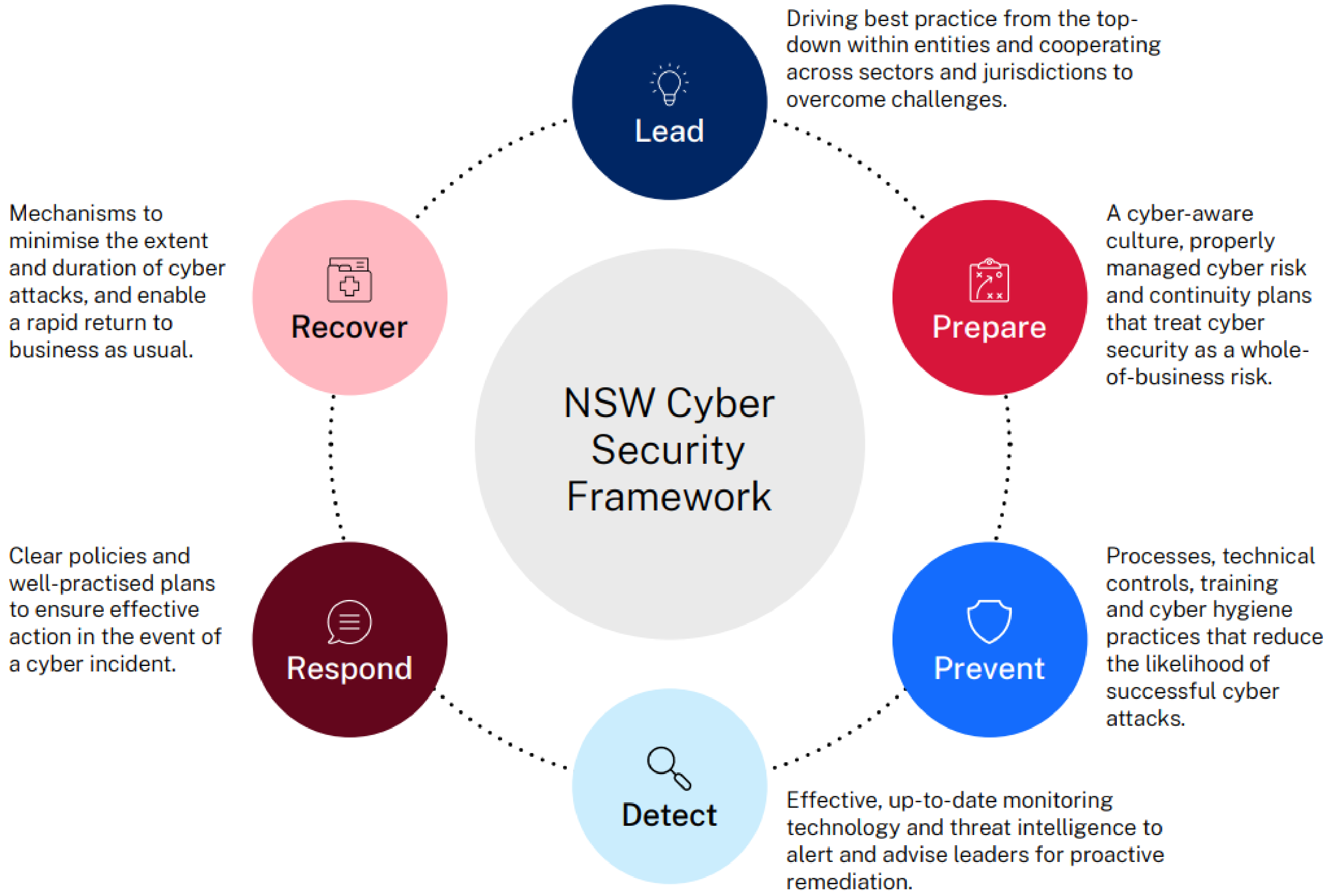
Cyber Security NSW Service Catalogue



Department of Customer Service

Cyber Security NSW Service Catalogue

January 2024



NSW Cyber Security Framework

Lead

Driving best practice from the top-down within entities and cooperating across sectors and jurisdictions to overcome challenges.

Prepare

A cyber-aware culture, properly managed cyber risk and continuity plans that treat cyber security as a whole-of-business risk.

Prevent

Processes, technical controls, training and cyber hygiene practices that reduce the likelihood of successful cyber attacks.

Detect

Effective, up-to-date monitoring technology and threat intelligence to alert and advise leaders for proactive remediation.

Respond

Clear policies and well-practised plans to ensure effective action in the event of a cyber incident.

Recover

Mechanisms to minimise the extent and duration of cyber attacks, and enable a rapid return to business as usual.

Cyber Security NSW Service Catalogue

Security assessments

Identify cyber security strengths and areas requiring improvement and understand how to bolster cyber security protections accordingly.

Awareness and training

Increase cyber security awareness and understanding among staff and contractors and improve organisational resilience.

Advice and guidance

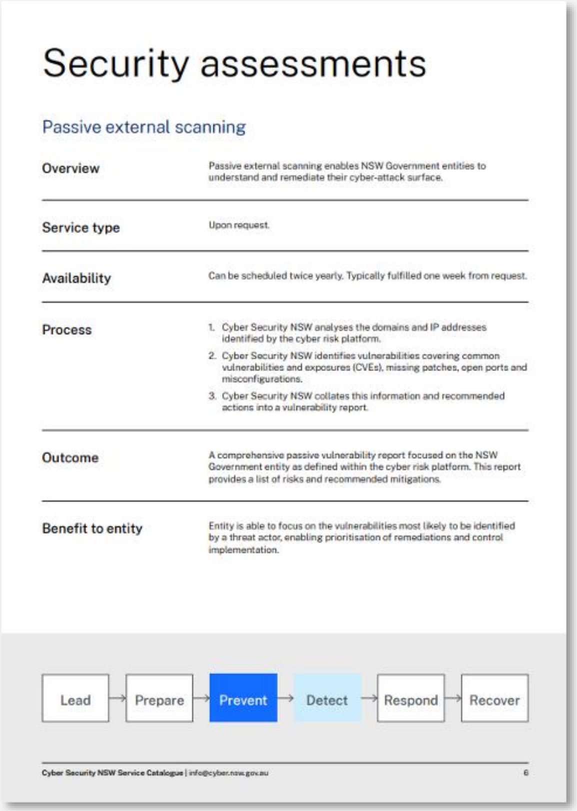
Obtain expert advice on risk, implementation of the NSW Cyber Security Guidelines and cyber security matters.

Threat intelligence

Receive proactive and targeted intelligence, as well as recommended mitigations, to enable early warning and action for likely threats in the NSW context.

Incident response

Be supported when cyber security incidents occur. Cyber Security NSW can assist with incident response, coordination, initial investigation and digital forensics.



Security assessments

Passive external scanning

Overview	Passive external scanning enables NSW Government entities to understand and remediate their cyber-attack surface.
Service type	Upon request.
Availability	Can be scheduled twice yearly. Typically fulfilled one week from request.
Process	1. Cyber Security NSW analyses the domains and IP addresses identified by the cyber risk platform. 2. Cyber Security NSW identifies vulnerabilities covering common vulnerabilities and exposures (CVEs), missing patches, open ports and misconfigurations. 3. Cyber Security NSW collates this information and recommended actions into a vulnerability report.
Outcome	A comprehensive passive vulnerability report focused on the NSW Government entity as defined within the cyber risk platform. This report provides a list of risks and recommended mitigations.
Benefit to entity	Entity is able to focus on the vulnerabilities most likely to be identified by a threat actor, enabling prioritisation of remediations and control implementation.

Lead → Prepare → Prevent → Detect → Respond → Recover

Cyber Security NSW Service Catalogue | info@cyber.nsw.gov.au 6

Cyber Security Strategy and Documentation

***1.4** Develop and maintain a cyber security strategy.*
***1.5** Develop and maintain formalised plans, policies and processes for cyber security practices.*

Cyber Security Strategy

- Aligns with the broader business objectives
- Captures key threats, vulnerabilities and risks facing the organisation
- Initiatives to uplift cyber security gaps and capabilities.

Benefits of formalised cyber security practices include:

Stakeholder communication

Guide technology investment

Reputation and trust

Resources

Cyber Security NSW has a range of products and tools available to aid implementation of the Policy's Mandatory Requirements.

Service Catalogue

Best practice cyber security advice

NSW Cyber Security Policy guidance

Maturity uplift assistance

Community of Practice

MS Teams Channel

Assortment of templates:

- Cyber Security Plan Template and Guidance
- Local Government Guidelines

If you don't have access, please contact community@cyber.nsw.gov.au

Govern & Identify

Govern & Identify

Risk Management

1.9 *Define risk tolerance, risk appetite, and manage cyber security risk.*

1.10 *Identify and manage third-party service provider risks, including shared ICT services supplied by other NSW Government agencies.*

Cyber Risk Framework

- Cyber risk management is integral to safeguarding an organisation's systems, data, and maintaining operational continuity and must be included in risk assessments.
- A risk-based approach to cyber security will tailor security measures to the specific threats and vulnerabilities faced by your organisation.

Benefits of risk management include:

Resource optimisation

Third-party due diligence

Executive oversight and accountability

Resources

Cyber Security NSW has a range of products and tools available to aid implementation of the Policy's Mandatory Requirements.

Service Catalogue

- Strategic Cyber Security Contract Advice
- Vendor Security Risk Assessment
- ACSC Vulnerability Data
- Vulnerability Risk Management Platform
- OSINT
- DMARC Support
- Key Website Monitoring

Community of Practice

MS Teams Channel

- Cyber Risk Management Toolkit
- Cloud Guidance

If you don't have access, please contact community@cyber.nsw.gov.au

Incident Response, Recovery and Reporting

2.2 *Maintain a cyber incident response plan and use exercises and post incident reviews to continuously improve the plan.*
2.3 *Report cyber incidents and provide information on threats to Cyber Security NSW.*
2.4 *Include cyber security in business continuity (BCP) and disaster recovery (DR) planning.*

Incident Response

- It is simply not enough to respond to incidents; equal significance must be placed on maintaining operations during and after disruptions, along with a commitment to continuous improvement to review, test and update these living documents.

Benefits of Incident Response, Recovery and Reporting include:

Demonstrated leadership	Interagency collaboration	Community wellbeing

Resources

Cyber Security NSW has a range of products and tools available to aid implementation of the Policy's Mandatory Requirements.

Service Catalogue

Exercise-as-a-Service (EaaS)

Build-an-Exercise

Community of Practice

MS Teams Channel

Cyber Security Incident Response Plan Template and Guidance:

- Checklist
- Example resources

Notification requirements and reporting Template

Cyber BCP and DR Guidance and Checklist

If you don't have access, please contact community@cyber.nsw.gov.au

Cyber Security Culture & Awareness

***3.1** Conduct awareness activities, including mandatory awareness training.*

Cyber Security Awareness

- Organisational leadership sets the tone for its cyber security culture. Commitment and active involvement in promoting a security-conscious environment is essential for creating a culture of cyber security awareness and preparedness.

Benefits of cultivating a cyber-first culture include:

Empowering employees

Cyber resilience investment

Foster behavioural change

Resources

Cyber Security NSW has a range of products and tools available to aid implementation of the Policy's Mandatory Requirements.

Service Catalogue

Cyber Security Awareness Training (Live & e-Module)

Community of Practice

MS Teams Channel

Awareness materials

Awareness campaigns

Community of Practice Forums

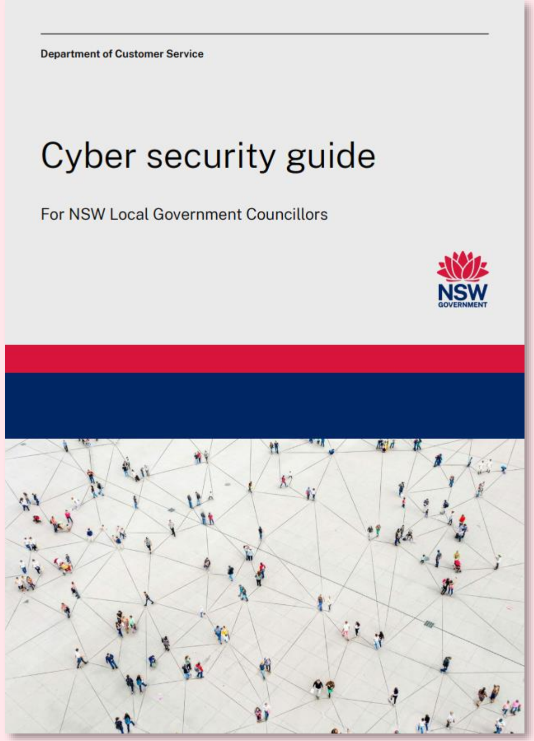
Adaptable training deck

If you don't have access, please contact community@cyber.nsw.gov.au

Protect

Resources for Councillors

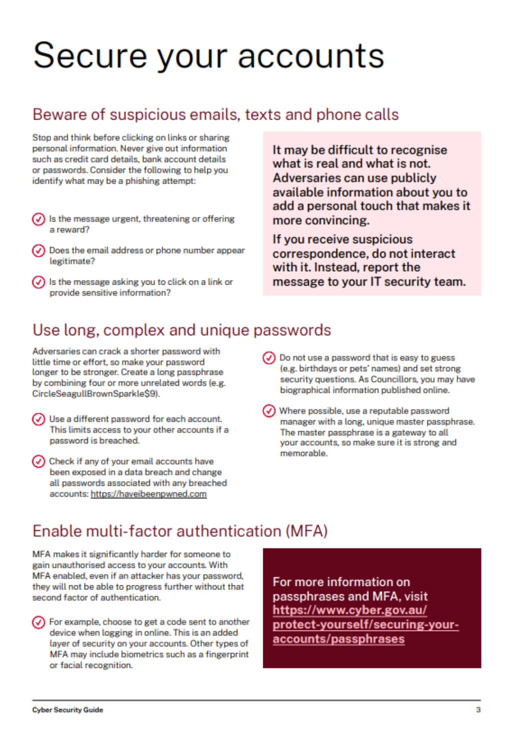
Cyber Security Guide for NSW Government Councillors



Department of Customer Service

Cyber security guide

For NSW Local Government Councillors



Secure your accounts

Beware of suspicious emails, texts and phone calls

Stop and think before clicking on links or sharing personal information. Never give out information such as credit card details, bank account details or passwords. Consider the following to help you identify what may be a phishing attempt:

- ✓ Is the message urgent, threatening or offering a reward?
- ✓ Does the email address or phone number appear legitimate?
- ✓ Is the message asking you to click on a link or provide sensitive information?

It may be difficult to recognise what is real and what is not. Adversaries can use publicly available information about you to add a personal touch that makes it more convincing.

If you receive suspicious correspondence, do not interact with it. Instead, report the message to your IT security team.

Use long, complex and unique passwords

Adversaries can crack a shorter password with little time or effort, so make your password longer to be stronger. Create a long passphrase by combining four or more unrelated words (e.g. CircleSeagullBrownSparkle$9).

- ✓ Use a different password for each account. This limits access to your other accounts if a password is breached.
- ✓ Check if any of your email accounts have been exposed in a data breach and change all passwords associated with any breached accounts: https://haveibeenpwned.com
- ✓ Do not use a password that is easy to guess (e.g. birthdays or pets' names) and set strong security questions. As Councillors, you may have biographical information published online.
- ✓ Where possible, use a reputable password manager with a long, unique master passphrase. The master passphrase is a gateway to all your accounts, so make sure it is strong and memorable.

Enable multi-factor authentication (MFA)

MFA makes it significantly harder for someone to gain unauthorised access to your accounts. With MFA enabled, even if an attacker has your password, they will not be able to progress further without that second factor of authentication.

- ✓ For example, choose to get a code sent to another device when logging in online. This is an added layer of security on your accounts. Other types of MFA may include biometrics such as a fingerprint or facial recognition.

For more information on passphrases and MFA, visit https://www.cyber.gov.au/protect-yourself/securing-your-accounts/passphrases

Cyber Security Guide 3

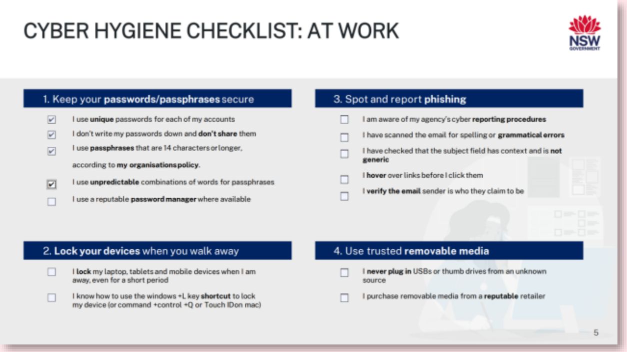
https://www.digital.nsw.gov.au/sites/default/files/2024-03/Cyber-Security-Guide-for-NSW-Local-Government-Councillors.pdf

Resource Pack

Resources for Councillors

Cyber Security NSW

A cyber safe NSW: connected, protected & trusted.



CYBER HYGIENE CHECKLIST: AT WORK

1. Keep your passwords/passphrases secure

- ☑ I use **unique** passwords for each of my accounts
- ☑ I don't write my passwords down and **don't share** them
- ☑ I use **passphrases** that are 14 characters or longer, according to **my organisations policy**.
- ☑ I use **unpredictable** combinations of words for passphrases
- □ I use a reputable **password manager** where available

2. Lock your devices when you walk away

- □ I **lock** my laptop, tablets and mobile devices when I am away, even for a short period
- □ I know how to use the windows +L key **shortcut** to lock my device (or command +control +Q or Touch IDon mac)

3. Spot and report phishing

- □ I am aware of my agency's cyber **reporting procedures**
- □ I have scanned the email for spelling or **grammatical errors**
- □ I have checked that the subject field has context and is **not generic**
- □ I **hover** over links before I click them
- □ I **verify the email** sender is who they claim to be

4. Use trusted removable media

- □ I **never plug in** USBs or thumb drives from an unknown source
- □ I purchase removable media from a **reputable** retailer

5

Key takeaways

Know your risks

Understand the threat landscape

Know where to find resources

Report cyber events and incidents

Further resources

Who?	When / why?	How?
Cyber Security NSW	Your Council security team can work with Cyber Security NSW on high-level cyber security strategy, policy and standards as well as incident reporting, coordination or advice.	General: info@cyber.nsw.gov.au Awareness: community@cyber.nsw.gov.au Incident Reports: report@cyber.nsw.gov.au
ID Support NSW	Provides identity theft advice and support, including how to restore the security of your identity if your government-issued proof of identity credentials are stolen or fraudulently obtained (i.e. drivers licence, birth certificate).	https://www.nsw.gov.au/idsupport-nsw **Phone:** 1800 001 040 Mon-Fri 9am-6pm **Online Form:** https://www.nsw.gov.au/idsupport-nsw/contact-idsupport
ReportCyber (ACSC)	If you are the victim of a cyber crime, you can report to ReportCyber (a branch of the Australian Cyber Security Centre). Covers individuals, businesses/organisations and government.	https://www.cyber.gov.au/acsc/report 1300 CYBER1 (1300 292 371)
eSafety	Leads and coordinates the online safety efforts of government, industry and the not-for-profit community in Australia. eSafety helps safeguard Australians at risk from online harms and promote safer, more positive online experiences.	https://www.esafety.gov.au/
Scamwatch	Scamwatch is run by the Australian Competition and Consumer Commission (ACCC). It provides information to consumers and small businesses about how to recognise, avoid and report scams.	https://www.scamwatch.gov.au/report-a-scam

Thank you

Any questions?

You can contact us at info@cyber.nsw.gov.au