Department of Customer Service

# Cyber security guide

For NSW Local Government Councillors

# Overview

**Cyber Security NSW leads, implements and supports cyber security initiatives to achieve the vision of a cyber-secure NSW. To assist councils in improving their cyber security maturity, Cyber Security NSW delivers a wide range of products, and services, along with best practice advice and guidance.**

## Cyber Security Guidelines for Local Government

Cyber Security NSW has developed Cyber Security Guidelines for Local Government (Guidelines) in collaboration with the Office of Local Government (OLG).

The Guidelines are based on the NSW Cyber Security Policy which outlines mandatory requirements to ensure key cyber security risks are appropriately managed.

Reporting maturity against the Guidelines is not currently mandated, however councils are encouraged to assess and report their progress to Cyber Security NSW.

For more information on the Cyber Security Guideline - Local Government, visit https://www.olg.nsw.gov.au/council-circulars/22-39-release-of-cyber-security-guidelines-for-nsw-local-government/

For more information on the Cyber Security NSW Local Government Engagement Plan, see under Cyber Security NSW Circulars at https://www.digital.nsw.gov.au/delivery/cyber-security/policies

## How cyber security impacts your role as a Councillor

Your Council's cyber security will be managed on a day-to-day basis by the Council Officers. However, as leaders it is important you ensure cyber security risks are appropriately identified and managed, and that processes are in place protect your organisation. This guide provides security advice to support you and your staff from threats, including:

### Social engineering

attacks that aim to manipulate people to provide confidential or personal information, which can be used for fraudulent purposes. There are many forms, the most common being phishing.

### Identity theft

when personal information – such as driver licences, passports and bank details – is accessed and used without consent. This information may be used to steal money or commit fraud.

### Ransomware

attacks that use malicious software to make data or systems unusable until the victim pays a ransom. It is NSW Government policy never to pay a ransom, as it can encourage further cyber attacks.

# 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**

# Secure your devices

## 01

### Manage multiple devices securely

As a Councillor, you are likely to be issued multiple digital devices to perform your duties. Ensure you manage these devices securely.

- ✓ Avoid sharing your official devices with others to reduce the risk of sensitive information being inappropriately accessed.
- ✓ Avoid signing into your accounts on someone else's device to reduce the risk of sensitive information being synchronised to their device.
- ✓ Use your work account for work purposes only, and your personal accounts for personal use only. Ensure you use different, unrelated passwords between both accounts.

## 02

### Restrict the sensitive information your applications can access

Software and applications can ask for permission to access information, such as your location, contacts, camera, files and microphone.

- ✓ Consider restricting these permissions in your privacy settings, even for well-known software and applications.
- ✓ Only use reputable software and applications downloaded from trusted app stores and websites.
- ✓ Regularly assess the applications on your devices and delete the ones you no longer use.

## 03

### Lock your devices and never leave them unattended

Never leave your devices unattended. If you are stepping away from your desk, lock your screen with a unique passphrase or biometric, such as facial identification or fingerprint scanning.

## 04

### Enable automatic software updates

Cybercriminals actively scan the internet for devices that are running vulnerable software versions. Enable automatic updates for all digital devices – including smart TVs, smart watches and anything connected to the internet – to benefit from the latest security features.

## 05

### Back up important files

Protect your important information by regularly backing it up.

Backing up your files lets you recover your information if it is ever lost, stolen, compromised by malicious software or damaged.

- ✓ Back up data to the cloud or another secure and known external storage device.
- ✓ Only use storage devices from reputable sources. If you find a USB or external hard drive lying around, never plug it into your device, as it could contain hidden malware.

# Secure your social media

## Check your privacy settings and what is publicly visible

Be mindful of what you post as criminals can use social media to perform reconnaissance against local government figures. Review your privacy settings regularly, as these often fluctuate.

## Keep your social media accounts secure

Be cautious when approving connection requests from other accounts, especially if they have an unusually low number of posts, pictures or connections.

Use a search engine to look for any publicly visible old photos or social media accounts. If you are not happy with the amount of personal information visible, adjust the privacy settings or delete old social media accounts you no longer use.

Be mindful when signing up to sites using your social logins such as Google, Facebook or Twitter. If breached, attackers can gain access to all services authenticated via that social account.

Use strong unique passphrases for separate accounts and enable MFA where possible. Only verify account requests or login attempts if you made the request.

Avoid sharing sensitive personal information and educate your friends and family who may be sharing too much. Small pieces of information can be put together by adversaries to form a picture about you for identity theft, or to guess account reset questions or login details.

Separate your public and private life by creating separate official and personal social media accounts for the information you share with different audiences.

Avoid sharing login details for social media accounts. If staff need to manage your social media accounts, there are secure ways to share access such as corporate accounts with multiple users.

**Be mindful of what you share online – could where you live or where your children go to school be identified from your posts? Personal information can be used to inform social engineering attacks, directed at you or your contacts.**

# Secure your communication

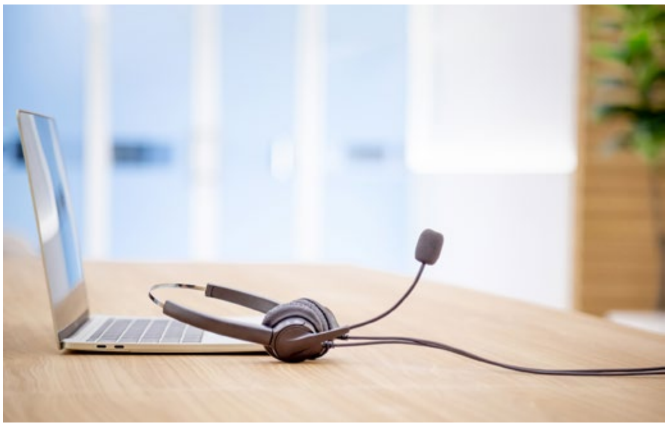
## Enable security features within messaging applications

Protect your messages from being intercepted by adversaries. You should not trust Signal, WhatsApp or other messaging software or applications with classified data.

**Be cautious when using group messages as there are more opportunities for information to be compromised with larger groups. Not all applications offer end-to-end encryption for group messages.**

## Only share official information on official devices

Only official devices have the right security protections in place to protect official information.



## Secure your video calls

Only share meeting invitations via private channels such as email or messaging applications to avoid unwelcome guests. Regularly update meeting login details and access links so that previous members cannot access meetings without an invitation.

Join meetings from a private location whenever possible. If there are other people nearby, it is best practice to be mindful of eavesdropping and use headphones so that only meeting participants will hear the full conversation.

Point your webcam away from any sensitive information in your background and always unplug or cover webcams when not in use.

Be careful when sharing your screen. It is best practice to only share specific software or applications instead of your entire screen.

# Secure your travel

## Never use public wi-fi for official devices

Public wi-fi is insecure and can expose your internet activity to monitoring by cybercriminals. When you are travelling or working remotely, set up a personal mobile hotspot rather than using public wi-fi. Disable wi-fi, Bluetooth, GPS, near field communications (NFC), cellular and any other connectivity functions.

## Avoid leaving devices unattended

One of the biggest risks to your information is from lost or stolen devices. Know where your devices are at all times when travelling, and enable encryption if your device supports it.

- ✓ Develop the habit of using keyboard shortcuts to lock screens whenever you step away from your device, even for a moment.
- ✓ Use the 'find my device' function, or the ability to remotely erase your information to provide additional security in the event of loss or theft.

## Overseas use of your devices

Your devices may be more susceptible to targeting by adversaries when you travel.

Speak to your IT team early when preparing to travel, as you may need to use dedicated 'clean devices' and accounts to limit the information that can be accessed from your devices if compromised, lost or stolen.

Have hard copy contact details ready for who to contact in case your device is compromised, lost or stolen.

It is best practice to wait until you are home before posting anything on social media that gives away your location.

# Support available for your Council

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 sets out a strategic approach to local government sector engagement.

## Principles of engagement

### Purposeful

Cyber Security NSW will focus on clearly defined objectives from initiation of each engagement. Engagement will rely on who we need to engage, understand desired outcomes, and most effective ways to reach those outcomes.

### Inclusive

Engagement will enable all NSW local government entities to participate, regardless of size, location and cyber security maturity. A flexible approach to engagement ensures the inclusion of all NSW local government entities.

### 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.

### Respectful

Cyber Security NSW acknowledges and respects the expertise, perspective and needs of NSW local government entities. Our engagement will be open to alternative views and ideas. Communication needs and preferences will also be adapted to NSW local government entities wherever possible.

### Transparent

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

### Prioritised

Engagement with NSW local government entities is prioritised to ensure outcomes are realistic, achievable and supported throughout the engagement.

### Tailored

Through consultation, our approach will be tailored to each unique environment and circumstances to enable the most efficient and productive service offerings for each NSW local government entity.

**More information on the methods of engagement and streams of engagement can be found in the Cyber Security NSW Local Engagement Plan. To access the plan, see under Cyber Security NSW Circulars at https://www.digital.nsw.gov.au/delivery/cyber-security/policies**

# Key products and services

### 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 Policy 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 incidents occur. Cyber Security NSW can assist with incident response, coordination, initial investigation and digital forensics.

**NSW Government entities can contact info@cyber.nsw.gov.au to request, or find out more about, the products and services detailed in this document.**

Department of Customer Service

**Contact details:**
If you think you have been a victim of a cyber attack, your first point of contact should be your organisation's IT Service Desk. Keep their details handy in case you lose access to your devices.

If you think you have been a victim of identity theft, reach out to:

**ID Support NSW:**

1800 001 040

idsupport@customerservice.nsw.gov.au

For more information, contact:

**Cyber Security NSW:**

info@cyber.nsw.gov.au

NSW GOVERNMENT