NORTHERN MIDLANDS COUNCIL
POLICY MANUAL

INFORMATION TECHNOLOGY SECURITY

Originated Date:	Adopted 20 January 2020 – Min. No. 015/20
Amended Date/s:	Revised 20 January 2025 – Min. No. 25/0034
Applicable Legislation:	*Privacy Act 1988* *Privacy and Other Legislation Amendment Bill 2024*
Objective	Safeguarding the organisation's technology environment, mitigating risks, ensuring regulatory compliance and maintaining operational continuity.
Administration:	Corporate Services
Review Cycle/Date:	Every 4 years, to be reviewed 2028.

1. PURPOSE

Northern Midlands Council takes the security of our network very seriously, and puts significant effort into mitigating the risks inherent in today's online world.

However we also recognise that security is a balancing act between eliminating all risk and unnecessarily stringent protocols which could cause a significant impact on the day to day productivity of staff and visitors.

2. APPLICATION

Accordingly our standard procedures for information security include the following measures:

- All inbound and outbound traffic is inspected by our stateful packet inspection firewall to monitor for suspicious traffic and detect potential attacks as early as possible;
- Internet traffic is logged and monitored, both to limit user's ability to reach malicious/compromised websites, but more generally to ensure that in the event a user's internet activity is having a significant impact on their own or other's productivity that the behaviour can be managed;
- Inbound email traffic is proactively filtered for spam and malware, and URLs in emails proactively checked to limit the risk of users inadvertently clicking through to malicious websites. All email is archived in a third party system to prevent users from permanently deleting council information, whether inadvertently or with malicious intent;
- All of NMC's on premises data is backed up regularly (at a minimum, daily) in multiple diverse locations to protect from data loss;
- Any of NMC's data that is stored off premises (e.g., in the cloud) is subject to checks for security and backup compliance; and
- Where possible, two factor authentication is enabled for all staff accounts.

3. DATA BREACHES

Any individual who suspects that a theft, breach or exposure of Northern Midlands Council data has occurred must provide a description of what occurred to their manager or to the IT Systems Officer as soon as practically possible.

The IT Systems Officer will investigate all reported thefts, data breaches and exposures, engaging specialist experts if required, to confirm whether a theft, data breach or exposure has actually occurred.

If a theft, data breach or exposure is found to have occurred, Northern Midlands Council will:

- Take steps to contain the theft, data breach or exposure to prevent any further compromise of personal information;

- Assess the theft, data breach or exposure of data and where possible, take action to remediate any risk of harm;
- Notify affected individuals, and where required under the Notifiable Data Breaches Scheme, also notify the Office of the Australian Information Commissioner; and
- Review the incident and consider what actions can be taken to avoid a reoccurrence of the theft, data breach or exposure.

4. DISASTER RECOVERY PLAN POLICY

Northern Midlands Council will maintain a separate Disaster Recovery Plan outlining the steps to be taken in the event of a disaster which destroys Northern Midlands Council's critical information technology infrastructure.

This Disaster Recovery Plan will be tested at regular intervals (ideally, every 12 months) to ensure that as far as practically possible, Northern Midlands Council's information infrastructure can be recovered to a functional state that allows Northern Midlands Council's critical services to continue operating within a reasonable timeframe. The definition of a reasonable timeframe will depend on the severity of the disaster.

5. IT RESOURCES DOCUMENTATION

Due to the extensive IT network operated by the NMC, IT Officers will document each piece of IT infrastructure, including updating such documentation when a piece is added, removed, or upgraded.

6. EMAIL POLICY (ELECTRONIC COMMUNICATIONS)

Information and Communication Technology Resources and Electronic Communications Acceptable Use Policy.

7. PASSWORD PROTECTION POLICY

Northern Midlands Council staff who require access to the corporate network will be provided a username and password to enable access to their allocated workstation/laptop and corporate applications.

Wherever possible, user passwords will be kept in sync with Northern Midlands Council's active directory so that a single password will provide access to all necessary systems. As this password enables access to privileged data, users must take all practical steps to keep this password secret. If a user suspects that an unauthorised third party has learned their password they must immediately change their password and notify the IT Systems Officer.

USER PASSWORDS MUST:

- Be a minimum of 14 characters long unless the user has Multifactor Authentication (MFA) setup, wherein the length will be 8 characters;
- Meet Microsoft complexity guidelines (contain characters from at least three of the following: upper case characters, lower case characters, numbers, non-alphanumeric characters, or Unicode characters that aren't upper case or lower case; and
- If an account does not have MFA, it must be ~~Be~~ changed on a regular basis. Policies will be maintained on Northern Midlands Council's network to enforce password changes at least every 190 days.

USER PASSWORDS MUST NOT:

- Be shared with other staff, except for the IT Systems Officer for the purpose of computer support and maintenance;
- Contain the names or birthdays of family members;
- Include any years between 1900 and the current year plus one, including two-digit representations (e.g., '94' for 1994)~~.~~;
- Be used for other non-council systems – it is important to use a unique password; and
- Be written down and stored in easily accessible locations (e.g. sticky notes under keyboards) or sent via insecure methods such as email.

8. REMOTE ACCESS POLICY

To enable access to network resources from outside Northern Midlands Network, remote access is available to staff. Generally this will be by means of a Virtual Private Network (VPN) connection into our network, with access controlled by the user's normal network username and password.

This access can be provided to staff on a case by case basis as needed by the IT Systems Officer. To ensure that the necessary security protocols are in place, generally this remote access will only be provided from a council owned device.

If remote access is to be provided to network resources using methods other than VPN then wherever possible this shall be locked down to specific IP addresses and not accessible from the open internet. Under no circumstances will remote access be enabled using risky or insecure methods such as direct RDP access from the internet.

Where possible, remote access must be accompanied by a Multifactor Authentication method. For example, staff access must have MFA, however a remote network resource, may not implement any MFA methods.

9. SERVER SECURITY POLICY

All servers on the Northern Midlands Council network are to have antivirus software installed and internet traffic filtered through a network firewall device.

Only the IT Systems Officer or authorised contractors will be provided with direct administrative access to servers. Authorised contractors will be issued with their own usernames and passwords, which will be given access rights under the concept of 'least privilege', ie the least access that is required to perform the functions that contractor has been engaged to perform.

10. SOFTWARE INSTALLATION POLICY

Computers provided to Northern Midlands Council staff will have all the necessary software installed for staff to perform their duties. No other software is to be installed on council devices without prior authorisation from the IT Systems Officer.

Staff will not be given local administrator privileges on their council owned computers unless there is a specific and important need for this access.

Installation of non-council approved applications on council smartphones is allowed, providing installation and use of the applications does not cause risk or disruption to the Northern Midlands Council network. If there is any doubt about whether the application may cause risk or disruption, staff must check with the IT Systems Officer before installing the application.

Council owned mobile devices (tablets/phones) are to be enrolled in Council's Mobile Device Management platform.

11. STAFF ONBOARDING / OFFBOARDING POLICY

ONBOARDING

When new staff who require IT systems access are employed at Northern Midlands Council, the People and Culture Business Partner will advise the IT Systems Officer in writing.

In order to provide the appropriate access, the IT Systems Officer will require, as a minimum:

- The new staff member's full name, position title, and commencement date;
- Information on what access is required, and what computer hardware will be used; and
- Information on what hardware may be required.

When access is created for the staff member, the IT Systems Officer will follow an onboarding checklist and document the access that has been provided in case it is required in future.

As soon as practical after the new staff member commences employment, the IT Systems Officer will perform a brief IT induction to impart a basic understanding of the software being used at the Northern Midlands Council and the acceptable use policies in place.

WHILE EMPLOYED

As a staff member takes on new duties that require additional accesses, these accesses must be recorded, and reviewed when a new employee takes on the same role.

OFFBOARDING

When staff members cease employment at the Northern Midlands Council, the People and Culture Business Partner will advise the IT Systems Officer in writing.

As soon as practical after the staff member's employment ceases, the IT Systems Officer will disable the staff member's user account and remove access to all council systems. To do this, the IT Systems Officer will follow a checklist of council systems to ensure no access remains enabled.

If the departing staff member had email access, their email account will either:

- Have an out of office message enabled to advise that the staff member has left employment with Northern Midlands Council; or
- Be forwarded to another staff member to be dealt with.

This email arrangement will remain in place for a grace period of at least 30 days, upon which time the email account will be disabled and unlicenced in Office 365.

11. WIRELESS COMMUNICATION POLICY

Access to the Northern Midlands Council corporate wireless network (network name 'NMC Staff') is for council provided / managed devices only, and access to this network is secured by means of an individual username and password that is allocated to each user. This is to ensure that devices have the appropriate security measures in place (for example antivirus software) before connecting to the network.

For all other devices, Northern Midlands Council provides wireless internet access via a wireless network 'NMC Guest' which provides internet access only and is segregated from the corporate network.

12. WORKSTATION SECURITY

Workstations and laptops on the Northern Midlands Council domain network will require a username and password for access. A disclaimer will be configured on the login screen of each device informing users that access is for authorised users only and is subject to the Northern Midlands Council Acceptable Use Policy.

Workstations and laptops must not be left unlocked when not in use, and a policy will be configured on the network to enforce an auto lock on devices after a period of inactivity.

All workstations and laptops supplied to staff by Northern Midlands Council will have antivirus software installed which is centrally managed by the IT Systems Officer. Other policies will also be enabled on the network to mitigate the risk of computer borne viruses and malware, including but not limited to:

- Software restriction policies that prevent unknown executables running from risky locations;
- Office policies limiting the use of macros; and
- Filtering of web and email traffic to limit access to malicious sites and files.