Information Security Policy

Policy Endorsement:	Endorsement Required by Executive Team		
Policy Superseded by this Policy:	Not Applicable		
Directorate:	Digital Technology		
Responsible Officer:	Chief Information Officer		
Policy Type:	Discretional		
File Number:	A2787714	Version No:	04
1st Adopted by EMT	30 June 2011	Last Adopted by EMT:	19 February 2025
Review Period:	Every 2 Years	Next Review:	May 2027

TABLE OF CONTENTS

1. POLICY OBJECTIVE (OR PURPOSE)

The integrity, confidentiality and availability of information technology resources are critical for the delivery of services to the City of Greater Dandenong.

The purpose of this policy is to ensure that measures are put in place to protect Council information and IT systems against security attacks and to mitigate the risks associated with unauthorised disclosure of information, while providing authorised users access to the information and data required to perform their duties.

IT systems and computing devices are essential tools in the day-to-day business activities of the Greater Dandenong City Council. They have increasingly become targets of malicious attacks by hackers, viruses and malware. In addition, inappropriate disclosure of information, particularly through the loss or theft of Council issued information devices, has the potential to cause harm to Council's customers and stakeholders and may expose Council to significant risks, both financially and to its reputation.

This document outlines principles and responsibilities for Council's DT staff and all users of DT systems and services. The objectives of this policy are compatible with the *Charter of Human Rights and Responsibilities Act 2006.*

2. BACKGROUND

In today's digital age, the City of Greater Dandenong relies heavily on information technology (IT) resources to deliver essential services to its community. The integrity, confidentiality, and availability of these resources are paramount to ensuring the smooth operation of the Council's functions and maintaining public trust.

The increasing sophistication of cyber threats, including hacking, viruses, and malware, poses significant risks to IT systems and computing devices. These threats can lead to unauthorized access, data breaches, and potential disruptions to services. Additionally, the loss or theft of Council-issued information devices can result in the inappropriate disclosure of sensitive information, causing harm to customers and stakeholders and exposing the Council to financial and reputational damage.

To address these challenges, this policy establishes a framework for protecting Council information and IT systems against security attacks. It aims to mitigate the risks associated with unauthorized disclosure of information while ensuring that authorized users have access to the data they need to perform their duties effectively.

This document outlines the principles and responsibilities for the Council's Digital Technology (DT) staff and all users of DT systems and services. The policy's objectives align with the *Charter of Human Rights and Responsibilities Act 2006*, ensuring that the Council's approach to information security respects and upholds human rights.

3. SCOPE

Who does it apply to?	This policy applies to all employees, Councillors, contractors, consultants and volunteers of the City of Greater Dandenong who have access to Council's technology resources and systems. It also applies to agencies and individuals who provide services to Council and will be made available to parties engaged under all relevant external supplier contracts.

This policy applies to all information systems and data owned, managed or operated by Council and to all computing and storage devices, either owned by Council or individuals, that are used to store, or access data owned by Council.

Computing and portable storage devices encompass a wide range of technology, including desktop computers, laptops, tablets, smartphones, USB devices, optical media (CDs and DVDs), flash drives, handheld wireless devices, wireless broadband cards, iPods, MP3 players, digital cameras, and any other devices capable of creating, accessing, distributing, or storing digital information

What happens if a breach occurs?

Breaching this policy may result in disciplinary action, performance management and review. Serious breaches may result in termination of employment or association. In the event the person is engaged via an external provider, consideration will be given to the remedies available under the service contract. This may include requiring the provider to replace the person delivering the services or termination of association with the service provider.

4. DEFINITIONS

User ID Login details assigned to a user to enable them to access systems such as username and password(s).

Encryption Process of converting data using an algorithm to a form that cannot be understood by unauthorised people. Usually authorised staff are given a key that allows them to decrypt the data to its original form.

LAN Local Area network, computer network at one site.

PSD Personal Storage Device, portable device with the ability to store data, e.g. digital cameras, external hard discs, USB devices.

Sensitive Information Information that should only be available to authorised persons, e.g. information protected under the *Privacy and Data Protection Act 2014*, personal details, credit card details, health records, financial information, etc.

This policy recognises that at times staff may send or receive sensitive information via personal email accounts that relates specifically to them. For example, a staff member may forward their payslip to a personal email account or an employee's roster may be sent to a personal email account. This is permitted under this policy providing the information does not breach the privacy of another individual.

Where data is shared with external bodies or consultants as part of Council activities this must be in accordance with relevant department procedures, e.g. data encryption for Financial Services information. Service agreements in place with external providers, including those developed and managed by the Procurement team, must always be followed to ensure the integrity and confidentiality of Council information.

Smartphone Mobile devices with a range of features beyond telephony, e.g. Internet access; Council's current smartphones are iPhone and Android. Other platforms will not be supported by Information Services. If this changes staff will be informed about systems as they are deleted or adopted.

Remote Access Gateway	Council's secure portal for accessing internal Council information and systems from external sites.
Strong password(s)	Passwords that cannot be easily guessed and contain digits, letters and special characters, as well as upper- and lower-case characters.
SSL	Secure Socket layer – A computer networking protocol that manages server authentication, client authentication and encrypted communication between servers and clients.
Wi-Fi	Ability of a computing device to connect to a wireless network.
CGD Application Portal	Council's secure portal for accessing internal web-based systems.
Phishing Resistant Authentication	To enhance council's organisation security posture, council implemented phishing-resistant authentication methods. These methods are designed to protect against phishing attacks, where malicious actors attempt to deceive users into revealing their login credentials. Specifically, council utilise FIDO2 standards, which employ cryptographic keys to validate user identities.
Endpoint detection & Response	To safeguard our council's digital assets and sensitive information, we implement Endpoint Detection and Response (EDR) solutions. EDR technology provides continuous monitoring and analysis of endpoint activities to detect and respond to potential cyber threats.
Geo-blocking	Geo-blocking is a technique used to restrict access to online content based on the user's geographical location. This is typically achieved by analysing the user's IP address to determine their location and then allowing or denying access accordingly.
Digital Technology	Digital Technology (DT) is the council IT services department

5. POLICY

When accessing Council owned information systems and data the following principles must be adhered to:

User access and passwords	Council provides authorised users with unique user IDs to access digital systems. Staff are responsible for maintaining the security of their passwords and for changing them as required by council policy. Any intentional disclosure of passwords to others will be deemed a breach of policy and may result in disciplinary action. If there is a need for someone else to access a user's account, DT staff will: 1. In the first instance determine if there is a solution which allows 'delegate' access (in order to maintain the integrity of the security records).

2. If delegate access is not an option, then DT staff will change the password(s) on written request (including reasons and period of access required) by the absent user's manager to do so. DT can support the manager regarding the security of data during this period. The user, who has had their password changed, will be notified of this by their Manager and DT as soon as practicable. The user is responsible for changing the password(s) on return to work.

Council does not permit the use of generic usernames and passwords for groups of staff as the audit trails of DT systems must be able to identify the user responsible for each transaction.

DT network administration staff are responsible for enforcing the expiry of passwords and the use of "strong" passwords by users.

All users accessing council resources remotely must utilize multifactor authentication (MFA) or phishing-resistant authentication methods. Additionally, internal council resources may also require multifactor authentication or phishing resistant authentication.

Anti-virus software or Endpoint Detection and Response (EDR) software

All data servers as well as Council owned desktop and laptop computers must have anti-virus or EDR software installed. DT staff ensure that subscriptions to anti-virus or EDR software are up-to-date.

DT staff ensure that users are not able to execute programs from PSDs. This eliminates a major source of virus infiltration.

Users are required to use council-owned devices to connect to the council network. Private computers are not authorised to access council's network.

Remote network access

Since the introduction of the Council Work from Home policy, staff can work remotely with a council authorised device in accordance with the work from home policy. Staff are required to be in Australia, provide a suitable internet speed to work from home and download security updates. Staff not located in Australia will be GEO blocked from accessing the council network remotely.

DDT staff ensure that Council devices have up-to-date anti-virus software, web filtering and hardened security practices applied.

DT staff enforce that remote access to Council's network can only occur using a Secure Socket Layer (SSL) connection. Staff must not store any Council owned sensitive data or passwords, unencrypted on PSDs or devices.

Storage device Control

All Council desktop and laptop computers must have storage device controls security measures implemented to ensure that only authorised storage devices can connect to a computer.

Privacy and confidentiality

In order to comply with Privacy obligations contained in the *Privacy and Data Protection Act 2014* all network users must ensure that the device on which they are accessing Council information does not pose any risks to breaches of privacy or confidentiality. This includes leaving confidential documents in accessible areas such as on printers. Further, when using a device, the user must ensure Council information cannot be accessed or

viewed by any unauthorised person including family or household members. Devices lock functions should always be used when a device is not being used and portable devices must not be left where they may be easily accessed or taken by others.

Users should note that the following practices have the potential to breach Council's policies as well as some legislation such as Privacy laws:

- Emailing Council information from or to a personal or non CGD issued email address.
- Creating, moving, saving or storing Council documentation or information (including information which relates to an individual such as a resident, rate payer or staff member) onto a non-issued CGD device.
- Connecting a non-approved device to CGD DT systems including printers, USB's, storage devices.
- Leaving an unattended PC or device with Council information logged on or accessible to unauthorised users.

- Staff are advised to exercise caution and avoid disclosing Personally Identifiable Information (PII) when using AI applications.

Data Breach Protocol

Greater Dandenong City Council is strongly committed to the transparent and responsible handling of personal and health information and to protecting every individual's right to privacy. Under the *Privacy and Data Protection Act 2014* and the *Health Records Act 2001*, Council is bound by the Information Privacy Principles and the Health Privacy Principles outlined in these pieces of legislation.

When Council is alerted to an alleged breach of its electronic systems or networks which store the personal or health information of individuals, Council's Information Privacy Officer will conduct a thorough and diligent investigation in accordance with Council's current Information Privacy/Data Breach Protocol.

Council's Information Privacy Officer also handles enquiries, complaints or adjustments regarding personal or health information and will respond to any query within 10 days of receipt unless the request is covered by the *Freedom of Information Act 1982*.

Storage repository

Information must be stored in the appropriate system, e.g. documents need to be stored in Council's Document and Records Management System

Users must ensure that they do not create, copy, move, save or store Council information outside the secure storage options provided by Council. For example, files must not be stored on personal or home PC's or devices used to access Council systems.

Information Transfer

Sharing of Council information should be via approved Council tools that provide a secure way to share and collaborate on documents. If this isn't practical, please consult DT regarding other acceptable options.

Removal of Assets

Equipment, information or software should not be removed offsite other than user's assigned devices. If required, an authority from Business Unit Manager in consultation with DT should be obtained.

Mobile computing and portable storage devices (PSDs)

Council staff and Councillors use a growing number of mobile devices, ranging from basic mobile phones to smartphones, tablet computers, laptops, digital cameras, optical media (CDs, DVDs and Blu Ray Discs) for data storage.

DT staff use a firewall to guard against viruses from remote computers and enforce the use of secure methods to access Council's systems (such as VPN or CGD applications portal).

To protect Council against the risk of disclosure of information to unauthorised recipients

- Users must not store Council owned data on mobile computing devices/PSD's. However, if there is no practical alternative to local storage, like remote access, all sensitive information/data must be stored on encrypted authorised tools approved by DT department
- Users must ensure that the information stored on mobile computing devices/PSD's is treated with the same care as that of hardcopy information and that all information stored on PSDs is handled in accordance with the *Privacy and Data Protection Act 2014* and *Health Records Act 2001*, the Greater Dandenong City Council Information Privacy and Records Management policies;

- Users must report the loss or theft of any CGD issued equipment including mobile devices or PSDs to DT as soon as possible. DT remotely wipe all data stored on mobile devices reported as lost or stolen and lock them to prevent unauthorised access
- Users must not send Council information, personal information or confidential data via email to their personal email address, as email is not a secure means of transferring information;
- Users must use security features available on the device such as passwords to protect their Council owned mobile computing devices, including smartphones, mobile phones and tablet computers

Physical security

Users must secure their mobile devices physically as much as practicable, e.g. lock them away if possible and not leave them unattended or on display, e.g. in parked cars.

Wi-Fi access

Council provides Wi-Fi access for staff, library patrons and the public in some Council buildings and the square outside the Dandenong Civic Centre. Access to the Wi-Fi network will be monitored to avoid abuse or inappropriate use of this facility.

Only staff with Council owned mobile devices can access Council's "Staff" Wi-Fi network, while the public can use the "Free Council Wi-Fi" network after accepting the terms and conditions. Presenting guests should be provided with a "Presenter Wi-Fi" guest account by the council staff they are meeting with.

Monitoring

DT staff and external incident response service provider will monitor any attempts to connect external computers to Council's network and analyse audit trails to identify suspicious activity. This is necessary to identify any systems or devices that may have been compromised by external parties.

Users agree to and accept that their access to Council's network may be monitored for this purpose.

Incident Response

To ensure our organisation is prepared for and can effectively respond to cybersecurity incidents, council utilises a third party for 24x7 Incident Response Service. This service offers around-the-clock support from a team of highly skilled incident response professionals and may disable staff or computer accounts to prevent or abate a cyber incident.

Software and application security Updates

DT staff will monitor and manage the deployment of security updates for Council software and applications to minimise Council's exposure to the threats facing the network e.g. malware, viruses, spam, etc.

Staff must authorise and apply security updates promptly. Devices that are not updated within the specified time frame will have the unsecure device network access revoked until the necessary security updates are installed. This measure ensures the security and integrity of our network and protects against potential vulnerabilities.

Identifying sources of threats

In order to maintain appropriate levels of security and respond to any potential threats to Council systems, users may be required to provide information on their CGD computer usage activities.

For example, if DT staff identify the potential source of threat as originating from a user's log in, Council may request information from the user regarding their activities around the time of the threat. Users are reminded of the importance of being open and honest in relation to providing this information to ensure the integrity of Council's systems is maintained.

Council strongly encourages all staff to actively use the "Report Phish" button. By doing so, you help prevent and mitigate potential cyber incidents, contributing to a safer and more secure work environment for everyone.

Access options

The Council aims to offer users a range of suitable options to access its systems, ensuring that business requirements are met while maintaining the highest levels of information security. This may include, but is not limited to, providing:

:

- Secure remote access such as VPN.
- Access to MyApps website
- Council issued devices that can be secured for remote use (smart phones and other mobile devices).
- Options for users to securely set up 'delegations' for periods of absence.
- Systems and processes (such as electronic document management system for document management) that allow other users to appropriately access shared information (e.g. Emails, documents etc.) relevant to carrying out their role.
- Data encrypted storage options where no other option is available

6. RESPONSIBILITIES

The responsibilities that arise under this policy are:

Role	Responsibilities
Users (including staff, Councillors and contractors)	• Must not disclose or share passwords • Keep passwords secure • Change their password(s) regularly. At a minimum when prompted by the system or immediately upon identifying a potential threat (including when it is known that another person knows the password(s)) • Use the security features such as password(s) and PINs to protect any mobile computing devices, including mobile phones • Lock or secure PCs or devices when not in use or when unattended • Must not store Corporate Data on PSDs • Report the loss or theft of any CGD equipment including mobile devices as soon as possible to the DT Service Desk.

	• Not use personal or non CGD issued email accounts to distribute Council information including information which relates to an individual such as a resident, rate payer or staff member. • Ensure that they make appropriate arrangement prior to planned periods of leave to ensure relevant business information can be appropriately accessed by those responsible for work in their absence. Information regarding setting delegation authority within systems is available from DT staff or on the intranet. • Provide information to DT staff as requested to assist them in ensuring information security is maintained. • At minimum all Council issued devices must be connected to the network monthly so any security updates can be applied. • Devices that are no longer in use should be reported to DT
Business Unit Managers	• Inform DT in a timely manner of any staffing changes, including extension and termination of employment contracts and change of roles • Review the list of users and their access rights provided by DT • Support users to put in place the necessary processes to cover work duties during periods of planned leave such as setting delegations in systems. • Ensure appropriate business processes are in place and systems are being used in accordance with Council procedures to reduce or eliminate the need to access a user's account when they are absent. • Authorise the removal of Assets in consultation with Senior DT Staff other than user assigned devices if required.
DT Department	• Enforce the use of strong passphrase • Ensure users to change passphrase regularly • Enforce security protection such as passphrase, PIN and biometrics on mobile devices • Enforce expiry of passwords • Manage installation and ongoing maintenance of anti-virus software • Maintain an SSL based solution for remote access and prevent any other form of remote access • Educate users where appropriate on options (such as delegations) that maintain data security and reduce the need for a user's account to be accessed or their password(s) to be changed in their absence. • So far as practicable, provide options that facilitate delivery of business requirements whilst maintaining information security • Acquire and secure USB drives through encryption, as authorised by the Records Management Coordinator on an individual basis • When a smart device is reported lost, wipe data stored on mobile devices and lock the devices immediately following their reported loss • Monitor access to Council's network and take appropriate actions to prevent potential threats or breaches to the system • Ensure that mobile devices and other equipment is configured to prevent loading of unauthorised software • Regularly monitor industry best practice and latest trends to ensure this policy remains relevant and effective • Authorise the removal of Digital Assets other than user assigned devices if required • All storage devices are wiped as part of the disposal process.

7. REPORTING, MONITORING AND REVIEW

To ensure the standards of this policy are met, Digital Technology will measure, conduct regular audits and assessments and monitor compliance with security protocols and identify potential vulnerabilities. Incident reporting mechanisms will be established, enabling staff to promptly report security breaches or suspicious activities. The success of the policy will be reviewed through periodic evaluations, including analysis of incident reports, audit findings, and feedback from users.

8. REFERENCES AND RELATED DOCUMENTS

Victorian Legislation, Principles and other reference sources (as amended or replaced from time to time)	• *The Charter of Human Rights and Responsibilities Act 2006* • *Crimes Act 1958* • *Health Records Act 2001*
Commonwealth Legislation, schemes and guidelines (as amended or replaced from time to time)	• *Crimes Act 1914* • *Privacy and Data Protection Act 2014* • *Freedom of Information Act 1982*