Digital Technologies Geelong

Network/Organisational Security Policy

1. Statement of policy

The purpose of this document is to ensure that appropriate measures are put in place to protect the systems, services and equipment of Digital Technologies Geelong and associated infrastructure.

The objectives of this policy are:

- To secure Digital Technologies Geelong's assets against theft, fraud, malicious or accidental damage, breach of privacy or confidentiality; and
- To protect Digital Technologies Geelong from damage or liability arising from the use of its Corporate Information Solutions (CIS) facilities for purposes contrary to Digital Technologies Geelong's Legislation and Policies.

The **Organisational Security Policy** determines how the CIS services and infrastructure should be used in accordance with ICT industry standards and to comply with strict audit requirements.

Digital Technologies Geelong adheres to the requirements of Australian Standard Information Technology: AS ISO/IEC 27001:2015 "Information technology—Security techniques—Information security management systems—Requirements"

As well as the relevant aspects of the "**Victorian Protective Data Security Framework**" (VPDSF), and the **Australian Cyber Security Centre (ACSC),** self-assessment document; "Strategies to Mitigate Cyber Security Incidents".

Following are broad requirements of the overall **Information Systems Security Policy**.

This Policy includes Access control; acceptable usage; logical security; data security; physical security; network security; business continuity.

2. Scope

This policy applies to all Digital Technologies Geelong staff, students, or any other persons otherwise affiliated but not employed by Digital Technologies Geelong, who may utilise Digital Technologies Geelong CIS infrastructure and/or access Digital Technologies Geelong applications with respect to the security and privacy of information.

3. Definitions

The following terms and abbreviations are specific to this policy:

Access Control: Control mechanisms and methods of limiting access to information resources to authorised users only. For example, passwords and user identification.
Application: A software package to perform a specific task (eg MS Word).
Authentication: The verification of the identity of a user based on for example, a password or Personal Identification Number (PIN) or a token.
Authorisation: The process of approving access to the Digital Technologies Geelong network, systems and information after the user has been adequately identified and authenticated.
Backup: A means of making a duplicate copy of a system and / or data for the purpose of being able to restore a system should a failure or corruption occur.
Bluetooth: A short range (10 meters) personal wireless connection of compliant devices.
Computer Work Area: Is an area or office in which access to computer resources is made available.
CIS: Corporate Information Solutions
DRP: Disaster Recovery Plan.

Firewall: A perimeter security device that controls IP traffic between the Digital Technologies Geelong internal networks and external networks. The firewall performs stateful packet filtering enabling the device to accept, reject or drop packets based on current firewall rules.
Gateway: An area on the Digital Technologies Geelong network where a connection to external sources such as the Internet exists. The Gateway is a barrier between the Internet and the internal network. It is responsible for filtering traffic, for example blocking requests from the Internet directed to the internal network.

ICT: Information & Communications Technology
Incident: An occurrence of suspect or illegal activity.
Infrastructure: All components that make up the computing facilities of Digital Technologies Geelong.
LAN: Local Area Network.
Patch: Software updates intended to remove or reduce risks from known vulnerabilities.
PC: Personal Computer.
Portable Device: Any handheld, or smaller, device used to access Digital Technologies Geelong systems or resources such as, but not limited to, iPhone, Smart phones, PDAs, iPad, mobile phones, laptop or notebook computers and the like.
SOE: Standard Operating Environment. This refers to the operating system and standard installed applications for a staff or student computer managed by CIS.
Users: Those who utilise the computing facilities of Digital Technologies Geelong.
User ID: Login details assigned to a user to enable them to use the ICT facilities.
Virus: A piece of code which is capable of copying itself and typically has a detrimental effect, such as corrupting the system or destroying data.
VOIP: Voice Over IP is a means of using the CIS network for transmission of voice phone calls.
VPN: Virtual Private Network.
WAN: Wide Area Network.
Wireless: Computer devices that connect using radio signals rather than cables.

4. Access control

This section specifies what is expected from staff, both permanent and contracted, and students alike as information security is the responsibility of all who utilise information technology services. The primary method of access is via Active Directory login, ie; username and password. Staff using their Digital Technologies Geelong credentials externally will require secondary authentication via Microsoft Azure Multi Factor Authentication (MFA).

In the case of staff, access to the network is granted at the time of account creation. This process is initiated by SHRD. Permission to network areas is granted based on AD group membership assigned by HR relevant to the role of the staff member.

4.1 Staff and student access

Digital Technologies Geelong provides students and staff with access to computing and communications services in support of its teaching, learning and administrative activities. These facilities include access to email, Internet, file and print services, an integrated data network across all campuses, Service Desk and Student computer classrooms and areas located across all campuses.

Users are responsible for maintaining the use and security of their assigned User IDs and all activity associated with that ID. **Knowingly disclosing passwords to others, or logging another user in with your ID, will be deemed a breach of policy and could be referred to disciplinary procedures.**

Digital Technologies Geelong expects its staff, students and associates to take all reasonable steps to ensure the integrity and security of Digital Technologies Geelong's ICT systems and data.

Where Digital Technologies Geelong staff require access to networks and systems outside the core Digital Technologies Geelong networks and systems the access will be granted on an "as needed" basis, that is, **access is granted to specific systems and to the level that is required to perform their duties.**

The principle of least privilege will be employed, including for specific security functions and privileged accounts. Non-privileged accounts or roles will be used when accessing non-security functions. The

Digital Technologies Geelong will prevent non-privileged users from executing privileged functions and audit the execution of such functions.

All Digital Technologies Geelong staff will be positively identified prior to gaining access to any Digital Technologies Geelong networks, systems and applications. This process requires that a Digital Technologies Geelong *Network User Account Authorisation form IS FO 03.01* be signed prior to account provisioning.

4.2 Strategic HR & Development responsibilities

It is the responsibility of Strategic HR & Development to ensure correct termination dates are entered into the HR system for staff terminations. The staff account will be **disabled** on the termination date and following a pre-determined number of days, the account will be **deleted**.

There are however, situations where an account may need to be disabled immediately and this can only be performed with the authorisation from the Executive Director, CIO, or delegated officer.

When Digital Technologies Geelong staff terminates their employment with The Digital Technologies Geelong confirmation must be received from the staff member’s manager that all computing equipment has been returned to Digital Technologies Geelong before final remuneration payments will be made. CIS also tracks assets via an asset management function to determine which equipment an individual has been assigned and thus must return on termination.

Keys and other access devices, such as authentication tokens and proximity cards, must be returned to Digital Technologies Geelong at this time.

All surplus, obsolete or replaced computer equipment must be returned to CIS for disposal. CIS is responsible for the disposal process. All computer equipment being sold, gifted or destroyed must have the hard disk drive rendered unreadable by the equipment owner prior to disposal.

4.3 Contract / temporary access

Employees such as temporary staff, contractors and consultants that require access to the Digital Technologies Geelong network and systems will be granted temporary access following written authorisation by the relevant Manager responsible for the contractor or temporary employee.

All temporary accounts will be assigned an account expiry date to coincide with the date that the temporary employee or contractor is expected to leave Digital Technologies Geelong or the date that they no longer require access to the Digital Technologies Geelong network.

Administrative level accounts will not be assigned to temporary employees and contractors. In the case of ongoing maintenance and support from 3rd party companies, access must only be granted to the relevant facilities within the system and be restricted to only the systems for which they provide support and for the period actual works are being carried out.

Generic network and system accounts will not be created unless approved in writing by the CIO or Manager, ICT Systems Infrastructure.

Where the use of a generic account has been approved, they will only be used on defined and limited networks and systems and will operate with limited functionality. Enhanced logging and monitoring may be performed on the use of generic accounts.

5. Acceptable usage

Identification of what is deemed acceptable (or unacceptable) usage of network, communication and Internet services.

5.1 Network usage

Digital Technologies Geelong provides students and staff with access to computing and communications services in support of its teaching, learning, research and administrative activities.

By signing the appropriate forms for obtaining access to Digital Technologies Geelong's computing facilities, or accepting the online compliance button, users agree to abide by all policies that relate specifically to the use of these facilities. Any breach of these policies will be deemed an infringement and dealt with accordingly which could result in suspension of access privileges or in severe cases, legal authorities will be involved.

Interfering, in any way, with Digital Technologies Geelong's network or associated equipment, be it intentional or accidental, is not permitted. Any such interference will be acted upon and may result in removal from Digital Technologies Geelong network until an investigation can be completed and the source of the interference is removed.

All usage must comply with the Digital Technologies Geelong's *Network User Policy.*

5.2 Electronic communications

Digital Technologies Geelong encourages staff and students to appropriately use electronic communication in order to achieve the mission and goals of Digital Technologies Geelong. Digital Technologies Geelong encourages the use of electronic communication to share information, to improve communication and to exchange ideas.

The electronic communications services must not be used for the distribution of material that may be deemed offensive, discriminatory or defamatory or the publishing or advertising of personal events or activities.

5.3 Internet usage

Use of Digital Technologies Geelong's computer network and public Internet and email facilities by Digital Technologies Geelong employees is permitted and encouraged where such use is suitable for business purposes and supports the goals and objectives of Digital Technologies Geelong. Digital Technologies Geelong Internet and email facilities are to be used in a manner that is consistent with Digital Technologies Geelong's standards of business conduct and as part of the normal execution of an employee's job responsibilities.

5.3.1 Appropriate use

Use of Digital Technologies Geelong Internet services will be consistent with the professional, legal, moral and ethical standards expected of Digital Technologies Geelong staff. Specifically, all use of Internet and email services will be:

- Lawful (In accordance with Australian and International laws).
- Appropriate for its purpose.
- Consistent with Digital Technologies Geelong policies and standards, State / Federal Government regulations.
- Able to undergo public and/or Digital Technologies Geelong scrutiny.

5.3.2 Unacceptable use

The following practices are considered unacceptable, and may be subject to disciplinary action as defined by Digital Technologies Geelong's "Staff Disciplinary Policy", including written warnings, revocation of access privileges, and, in extreme cases, termination of employment. Digital Technologies Geelong also reserves the right to report any illegal activities to the appropriate authorities.

- Viewing, downloading, storing, distributing or communicating information on the location of Internet sites that contain obscene or offensive materials.
- Sending or receiving any material that is obscene, offensive, inflammatory or defamatory, or which is intended to annoy, harass or intimidate another person.
- Accessing, downloading, and disseminating or using any program from the Internet that can be used to test the security of a system or compromise the security of a system.
- Soliciting e-mails that are unrelated to business activities, or soliciting non-Digital Technologies Geelong business for personal gain or profit.
- Representing personal opinions as those of Digital Technologies Geelong.

- Using the Internet or e-mail for gambling or illegal activities.
- Uploading, downloading or otherwise transmitting copyrighted material in violation of its copyright.
- Intentionally interfering with normal operation of the network, including the creation or distribution of malicious or harmful material in any form, such as computer viruses, or sustained high volume network traffic that substantially hinders others in their use of the network.
- Revealing or publicising confidential or proprietary information that includes, but is not limited to: Student/Customer Information, financial information and commercially confidential information.
- Examining, changing or using another person's files, output or user name without explicit authorisation.
- Intercepting or attempting to steal or alter information, unlawfully accessing, altering, or falsifying electronic documents or programs.
- Unauthorised access to a Website or other server accessible through the Internet and/or making unauthorised modifications to any public Internet site through hacking activity.
- Disseminating messages without authority that may cause people to fear for their safety or the safety of others.
- Intentionally intercepting, eavesdropping, recording, reading or altering another person's email messages.
- Other inappropriate uses of Internet/Intranet or network resources that may be identified by the network administrator.
- Tampering in anyway with computers, computer peripherals or network devices, this includes the unauthorised connection of any device to Digital Technologies Geelong network.
- The unauthorised installation of any software on to Digital Technologies Geelong computers or unauthorised access to any cloud-based application or service that could compromise the security and/or privacy of Digital Technologies Geelong's data.
- Deleting, or compromising, (or attempting to do either) any logging or monitoring software that exists in place to appropriately manage the network, user access and user activities.

5.3.3 Monitoring

The use of Digital Technologies Geelong's electronic systems and services is subject to monitoring to ensure secure operation, to investigate and diagnose and for identifying and investigating unlawful or inappropriate access and usage.

All usage must comply with Digital Technologies Geelong's *Network User Policy.*

5.4 Internet content filtering

Digital Technologies Geelong employs Internet Content Filtering technology as a tool in meeting its duty of care obligations by preventing access to inappropriate material including, but not limited to, adult content, gambling, and other sites deemed illegal or not appropriate for work when utilising Digital Technologies Geelong provided internet access.

5.5 Mobile devices

Mobiles devices including, but not limited to, laptop and netbook computers, mobile phones, smart phones and tablet devices, are all subject to the same policies and procedures as for other computing and communication devices.

6. Logical security

Implementing a suitable environment that protects the integrity, availability and confidentiality of Digital Technologies Geelong data by using logical or 'computerised' controls and processes.

6.1 Software security

Software security specifically relates to access rights and protection of software packages supplied by, and for the use by, Digital Technologies Geelong computer services infrastructure. All users of the network are supplied with a User Account for authentication and allocation of appropriate access rights to network facilities including software. Access to such network facilities and software is also controlled by the use of secure passwords

All Digital Technologies Geelong staff PCs and laptops must be set with an inactivity screensaver which requires a unique password to reactivate the underlying session and has a pre-set idle time.

As a means of allocating appropriate software packages to specific users, the use of an application deployment tool is used where possible. This can grant individuals or groups access to various programs and services in accordance to their duties and requirements through their user account.

6.2 Software development

Software development must only be performed in a controlled, test environment until such time that all flaws, bugs and potential vulnerabilities are removed. Only then can the developed software be managed through the Change Control process. Please raise a CIS Service Desk request stating as such.

Software development, should only be done where authorised by a member of the Executive team, and for the purpose of enhancing an existing application or meeting a need where no commercial software exists for the purposes required. There may also be instances where it is cheaper, faster or more appropriate to perform the in-house development.

Any software development that may cause harm or impact the IT resources of Digital Technologies Geelong in an adverse manner including, but not restricted to, scanning, gaining un-authorised access, exploiting vulnerabilities to take advantage of exploits, will be looked upon as inappropriate and treated as a direct attempt to compromise Digital Technologies Geelong’s computing facilities and / or infrastructure and will be dealt with accordingly.

6.3 End-point security and antivirus

All SOE Digital Technologies Geelong issued PCs and laptops have end-point security software installed. This is to ensure that the software is kept updated for the latest threats. There are also antivirus systems in place checking all incoming email into the institute and also on internally circulating emails. As of 2020, Digital Technologies Geelong uses CrowdStrike Falcon. This software utilises a cloud based monitoring service that also looks for behavioural patterns. Any computer suspected of compromise can be immediately isolated from the network for further investigation.

It is required that any non-SOE or Digital Technologies Geelong PCs and / or laptops also have current updated antivirus software installed, and it's the owners / users responsibility to ensure this. Not having current updated antivirus software installed exposes Digital Technologies Geelong systems and infrastructure to potentially significant disruption and damage due to virus infected computers.

6.4 Passwords

It is essential that those requiring access to Digital Technologies Geelong computing facilities be issued with a unique login and password. This password is not to be shared with, or used by, any other individual and failing to comply will be treated as a serious breach of system security which may result in disciplinary action.

Staff Passwords are to meet complexity rules as set by the current *Password Policy.*

In the event that access is required to Digital Technologies Geelong data that is held under a specific staff member’s user ID and password and that staff member is unavailable to access the data due to unforeseen circumstances, a request to have the password reset may be made with the authorisation of the CEO, CIO or delegated officer. This will only be considered when all other avenues to access the data have been exhausted. At the completion of the task accessing the required data, the password MUST be reset again and the staff member notified as soon as is practical.

Student Passwords are to also be set as required by the current *Password Policy.*

6.5 Patch management

To ensure that all Digital Technologies Geelong supplied end-user devices and applications are kept current and up-to-date, a central Patch Management Server is used. This server will send out any operating system and / or critical software updates, to Digital Technologies Geelong supplied PCs and laptops that are required to address any known software vulnerabilities. These updates will be distributed automatically.

It will be the responsibility of system administrators to ensure that the servers under their control are kept updated with required operating system and software updates and patches. Periodic checks will be performed on servers to assess their vulnerability status by the ICT Infrastructure manager in consultation with system administrators.

7. Data security

Ensuring that the confidentiality of data contained on the information technology systems is maintained and access is made available to those who are authorised to see that data. This section is also used in conjunction with confidentiality polices.

7.1 Confidential data security

To ensure the confidentiality and security of staff and student personal information contained on Digital Technologies Geelong's IT facilities, it is essential that only those authorised to access such data are permitted to do so. Business application owners are responsible for ensuring appropriate controls are in place to ensure users have suitable levels of access based on their business role.

Anyone, staff or student, who gains access to such personal information through methods other than those granted by completing the User Access Request Form, shall be deemed as unauthorised and subject to disciplinary action.

Staff should be aware of their legal and corporate responsibilities in relation to appropriate use, sharing or releasing of information to another party. Any other party receiving restricted information must be authorised to do so and that the receivers of the data also adopt information security measures to ensure the safety and integrity of the data.

7.2 Communications security

Communications can take various forms which include, but are not restricted to, voice via land line, voice via mobile phone, voice via computer network (VOIP), email, electronic file transfer, wireless access, Virtual Private Network (VPN) connections, dial up modem, Infra-Red, Bluetooth and IT network infrastructure.

Each of these communications methods poses its own unique security problems and needs to be addressed individually. In each case, where network communications is required, irrespective of type, only those methods as permitted by CIS will be allowed and must be in accordance with the specific Communications Security procedures which are developed to support this policy.

8. Physical security

Ensure that the physical ICT devices are kept safe from inappropriate access. This includes the physical access to the data centre/server room, switch and patch panel cabinets, and any other ICT devices in both restricted and public access areas

8.1 Asset control

All ICT devices over a value of $1000 must be registered with Digital Technologies Geelong's asset register. This also applies to the disposal of assets. CIS will control this process for all assets they procure but if ICT assets are procured outside of CIS, it is the responsibility of the person authorising that procurement to ensure CIS are updated on those assets so they can be added to the asset register.

8.2 Asset disposal

When disposing of ICT assets such as computers, laptops, printers etc, the disposal must be co-ordinated with CIS Technical Services to ensure that all data is removed using approved data removal tools and procedures. It is also a requirement that all software be removed prior to disposal to prevent potential breaches of software licence agreements.

8.3 Physical access security

All offices, computer rooms and work areas containing confidential information, or access to confidential information must be physically protected. This means that during working hours, the area must be supervised, so that the information is not left unattended, and after hours, the area must be locked or the information locked away.
It is a requirement that any PC / Laptop / Portable computer be logged out and turned off at the end of the working day unless a specific request is made to leave equipment turned on for the purpose of distribution of overnight processing is required.

Data Centres will be located at each physical site and will house all networking devices, such as Gateways, Firewalls, Core Switches and Servers. The Data Centres will contain monitored environmental controls including temperature, humidity, and fire detection and suppression controls as well as monitored security alarm systems.

Core Digital Technologies Geelong systems will be protected by an Uninterrupted Power Supply (UPS) and diesel powered generator to enable continuity of production data centre services in case of mains power failure.

Computer communications cabling used throughout the Digital Technologies Geelong will be housed inside cabling ducts within building walls and / or within approved cable conduit housing. Data Risers will be securely located inside locked communication cupboards or cabinets. Access to these communications cupboards will be restricted to specifically authorised CIS staff only, as approved by the CIO or the ICT Infrastructure manager

Where public (student) network access points exist, logical network controls will be used to restrict access to specific networks and systems.

8.4 Removal of equipment

Any Digital Technologies Geelong computer equipment, including laptops not specifically assigned to a staff member, will not be used off-site without appropriate authorisation of the staff member's relevant Manager.

Users shall exercise reasonable caution in using computer equipment away from Digital Technologies Geelong premises, such as when travelling. In particular, laptops will never be left unattended in a public place or visible in an unattended vehicle. Any equipment taken from a Digital Technologies Geelong campus without appropriate authorisation will be in direct violation of this policy and appropriate misconduct and / or legal action will be taken.

8.5 Lost or stolen computer equipment

Digital Technologies Geelong staff will report all lost or stolen Digital Technologies Geelong computing equipment to their relevant Manager who will take appropriate action. Managers will report any lost or stolen Digital Technologies Geelong computing equipment to Facilities by filling out an incident report. Facilities is responsible;

- For notifying Finance to initiate insurance claims and asset management
- Reporting the theft of the Digital Technologies Geelong computing equipment to the Police.
- Reporting to CIS, so appropriate records can be managed.

9. Network security

9.1 BYOD and wireless network

Digital Technologies Geelong does not current offer a wireless network.

9.2 Prohibited activities

- Peer-to-Peer networking is strictly prohibited on hosts connected to the Digital Technologies Geelong's network.
- The use of any unauthorized network interrogation utilities on the Digital Technologies Geelong's network is strictly prohibited.

10. Business continuity

10.1 Backup requirements

All major systems within Digital Technologies Geelong computing infrastructure are backed up on a regular basis. CIS have a Backup Strategy which details the frequency of backups. It is also strongly advised that all users save their work to their network drive as this drive is backed up and any loss or damage to files can often be rectified by the restoration of the files from an existing backup, refer to *Data back up Policy IS PO 05.*

10.2 Change control

To ensure that ICT facilities and services running within Digital Technologies Geelong infrastructure are maintained and kept running at maximum performance and functionality, it is often a requirement to perform maintenance and upgrades to equipment. To ensure that there is minimal disruption to essential services, appropriate Change Control procedures are to be followed. This is to ensure that the disruption is kept to a minimum and appropriate roll back procedures exist should there be issues during the system changes. Meetings of the Change Advisory Board (CAB) meet weekly for this purpose. CAB members review and approve or deny changes as required.

10.3 Disaster recovery plans

In the event of a disaster that impacts the computer infrastructure and / or services of the Digital Technologies Geelong's primary data center located at the city campus, the implementation of a Disaster Recovery Plan is essential. The DRP provides step by step procedures and processes required to ensure that services are returned to normal operation in the shortest possible time. The production and maintenance of such plans are the responsibility of the Enterprise Systems & Infrastructure manager. All procedures and processes should be tested and updated on a regular basis.

System owners will undertake business continuity planning for the information/systems that they own. The business continuity planning process will encompass the following components:

- Identification of critical systems and information
- Risk assessment
- Maintaining Business Continuity plans
- Training
- Testing
- Review

11. Breaches / infringements

Failure to abide by these terms will be treated as misconduct.

11.1 Minor infringements

For a first time offence of a minor infringement, a warning will be issued. Repeat offenses may be investigated as a serious infringement.

11.2 Serious infringements

A serious infringement may result in:

- Referral to the appropriate disciplinary procedures; and/or
- Referral to law enforcement agencies (where the infringement constitutes a legal offence).

12. Governance / responsibilities

Position	Governance / Responsibility
Managers	It is the responsibility of all managers to be familiar with Information Security Policies and their requirements and to ensure compliance by staff who report to them.
Chief Information Officer (CIO)	For the review and implementation of this policy and the maintenance of all associated documents.

13. Review and approval

	Position	Area
Author / reviewer:	Manager, ICT Systems Infrastructure	Corporate Information Solutions
Custodian:	Chief Information Officer (CIO)	Corporate Information Solutions
Endorsed by (if applicable):		
Ratified by (if applicable):		
Review schedule:	This policy will be reviewed every 3 years (or earlier as required)	
Last reviewed / updated:	27 October 2020	