Digital Technologies Geelong

Hardware/Software Policy

1. Statement of policy

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

The objective of this policy is:

- To ensure Digital Technologies Geelong's assets are fully functional and fit for purpose

The **Hardware/Software Policy** determines how hardware and software faults are tested, resolved and documented.

Following are broad requirements of the overall **Hardware/Software Policy**.

This Policy includes all hardware, software and networking equipment under the control of Digital Technologies Geelong.

2. Scope

This policy applies to all Digital Technologies Geelong staff, including temporary staff, contractors and consultants.

3. Definitions

The following terms and abbreviations are specific to this policy:

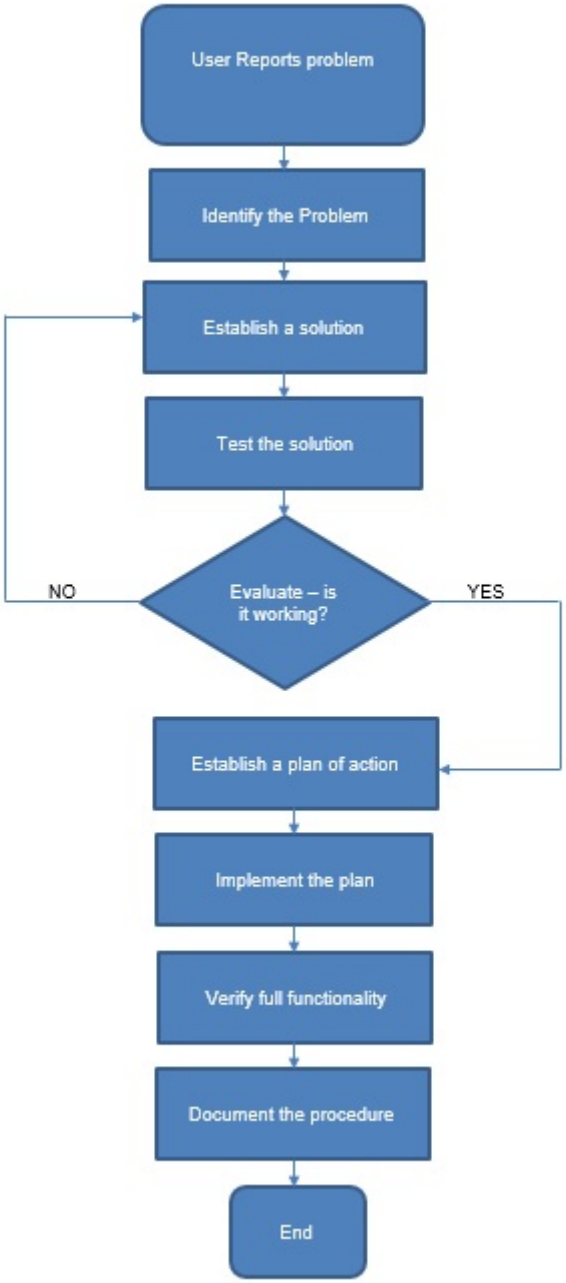
Access Control: Control mechanisms and methods of limiting access to information resources to authorised users only. For example, passwords and user identification.
Application: A software package to perform a specific task (eg MS Word).
Authentication: The verification of the identity of a user based 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.
osTicket: Open source support ticket system used by Digital Technologies Geelong to record all system support requests.
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. Testing Methodology

This section specifies what is expected from staff, both permanent and contracted, in testing and resolving problems with hardware, software and network connectivity.

4.1 .Gather information to identify the problem. This might be error messages, information from our users, or log files.
4.2 Enter details into Digital Technologies Geelong Help Desk tracking system, osTicket.
4.3 Using the osTicket knowledge base, check for possible resolutions to the problem and perform tests to see if this resolves the problem. If no similar problems have occurred, apply your knowledge of the system to identify and resolve the problem.
4.4 If the initial resolution doesn't resolve the problem, perform further tests until the problem has been resolved.
4.5 Once the problem is resolved, document the process for applying that resolution and apply to the production environment.
4.6 Verify that the system is working with the resolution that has been applied and notify the change control team or your supervisor that that the system is fully functional.
4.7 If this problem occurs again, refer to osTicket's knowledge base for details of the resolution that has been implemented.
4.8 Follow the flow chart to test, resolve and document problems related to hardware, software and network connectivity:



4.9 Staff responsibilities

All staff, including temporary staff, contractors and consultants, are responsible for using osTicket to report any hardware, software or network malfunctions.

5. Breaches / infringements

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

5.1 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.

5.2 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).

6. 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.

7. 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	