

POLICY DEVELOPMENT FRAMEWORK

ANTI-MALWARE

POLICY

Policy Number	Version 1.0
Date of Approval	November 2023
Policy Sponsor	Deputy Vice-Chancellor: Operations
Next Review Date	November 2026
Approver	Council
Department/Unit	CTS

TABLE OF CONTENTS

1. PURPOSE.....	3
2. SCOPE	3
3. OBJECTIVE AND CONTEXT	3
4. POLICY PRINCIPLE.....	4
5. COMMONLY USED TERMS & DEFINITIONS.....	5
6. ANSWERS TO FAQ.....	6
7. EFFECTIVENESS OF THE POLICY	7
8. RESPONSIBILITY.....	7

1. PURPOSE

1.1. The University is committed to ensuring effective protection of Information Assets, their contents, and systems which serve as paramount importance for the operations of CPUT, including systems that are hosted in the Cloud. Threats to the integrity, availability, and confidentiality of these Information Assets from within CPUT, third parties, or malicious persons external to CPUT can cause a significant impact on CPUT:

1.1.1. This policy aims to provide a comprehensive framework for implementing effective anti-malware protection measures within the university's computing facilities. It outlines the university's approach to safeguarding its systems.

1.1.2. Sets out the guiding principles and responsibilities to ensure the achievement.

2. SCOPE

2.1.1. This Policy applies to:

- 2.1.1.1. All employees, students, contractors, consultants, and temporary staff at CPUT, including those workers affiliated with third parties who have access to university information and computing devices.
- 2.1.1.2. All university-owned technologies and services, including systems hosted in the cloud, that are used to process university information.
- 2.1.1.3. External parties that provide information processing services to the university.

3. OBJECTIVE AND CONTEXT

- 3.1. Outline the organisations approach to anti-malware protection for university-owned technologies.
- 3.2. Establish clear principles and accountable responsibilities for all parties involved to ensure that the university's computing facilities are adequately secured and protected against malware threats.

4. POLICY PRINCIPLE

- 4.1. The anti-malware software supplied, managed, and owned by CPUT must be installed, run, and kept up to date on all university-owned computing devices, including those operating in the Cloud.
- 4.2. All systems built and/or hosted by third parties that are used by CPUT must run up-to-date anti-virus software installed on them.
- 4.3. To maintain the security of the CPUT network infrastructure, the CPUT IT department may monitor any system connected to the CPUT networked infrastructure for anti-virus software and may deny network access to any system/s without up-to-date anti-virus software until the software is installed.
- 4.4. Anti-malware protection software configured by the EUC department. must run regular (at least daily) scans on university-owned computing devices.
- 4.5. Users must be prevented from accessing known malicious websites through malware protection software or content filtering function.
- 4.6. Users are prohibited from disabling or modifying anti-malware software on university-owned computing devices. Any messages suggesting that antivirus protection has been disabled should be investigated immediately and reported to the IT Service desk department.
- 4.7. Appropriate detection and corrective controls must be in place to identify and minimise the impacts of malware infections that cannot be avoided or prevented by the other controls.
- 4.8. All university-owned computing devices must have the required operating systems and software updates installed in a timely manner. This is to ensure that the risk of exploiting known vulnerabilities is minimised.
- 4.9. Users must report any malware found on any university-owned technology, to the IT Service Desk Department
- 4.10. Computing devices that are deemed to be infected or posing a threat of propagating computer viruses and/or other malicious code will be disconnected from the CPUT network until the infection has been removed and the threat has been addressed.
- 4.11. Access will only be re-enabled once the device complies with the above requirements and is considered secure and free of malware. The root cause of the infection must be identified, and remedial actions must be taken to prevent a re-occurrence.
- 4.12. Failure and/or refusal to abide by the rules, principles and procedures detailed in this policy shall be deemed as misconduct and CPUT may initiate the appropriate investigation and disciplinary action against such individuals.

- 4.13. Penalties for violating this policy may include restricted access or loss of access to the CPUT network, institution of disciplinary proceedings which may lead to termination or expulsion, and in some cases, civil and/or criminal liability depending on the severity and frequency of the offence/violation.

5. COMMONLY USED TERMS & DEFINITIONS

- 5.1. **CPUT:** Cape Peninsula University of Technology which is the institution.
- 5.2. **POPIA:** Protection of Personal Information Act (POPI Act) No. 4 OF 2013.
- 5.3. **AVS:** Anti-Virus Software. Antivirus or anti-virus software (often abbreviated as AV). This is sometimes known as anti-malware software, or is computer software used to prevent, detect and remove malicious software.
- 5.4. **BYOD:** Personal devices like smartphones, laptops, and tablets that can access company resources and perform work-related tasks.
- 5.5. **Cloud System:** A collection of computing resources and services hosted on remote servers and accessed over the internet, allowing users to manage data and run applications without relying on local hardware infrastructure.
- 5.6. **Computing Devices:** Electronic devices that can process and store data or information using hardware and software components.
- 5.7. **CTS:** Computer and Telecommunication Services is the university's IT department which oversees the university's IT function with the CTS Senior Director being the head.
- 5.8. **CTS Management Team:** A group of individuals appointed by the company to oversee and make decisions on behalf of the organisation. The management team can include directors, managers, supervisors, and other leadership personnel.
- 5.9. **EUC:** End User Computing. This section is responsible for maintaining this specified policy. This section deals with systems such as Server Operating Systems, Desktops, Email Gateway, etc.
- 5.10. **IT:** Information Technology deals primarily with the utilisation, management, and enhancement of computer-based Information Systems.
- 5.11. **IT Systems:** Refers to physical servers, virtual servers, cloud hosted servers, end-user computing devices (laptops, desktops), and Mobile devices (phones, tablets,
- 5.12. **Malware:** Software that is specifically designed to disrupt, damage, or gain unauthorised access to a computer system. Computer viruses, network worms, Trojan horse programs, rootkits, key loggers, trapdoors, backdoors, adware, spyware,

crimeware, scareware, ransomware, Advanced Persistent Threats (APTs), etc. are collectively known as malware.

- 5.13. **Third-party suppliers:** Third-party suppliers are companies or individuals who provide products or services to a business or organisation but are not part of the organisation itself. These suppliers are external to the organisation and may be contracted to provide various goods or services.
- 5.14. **University-Owned Computing Devices:** Endpoint devices or Company-owned devices include desktop computers, laptops, servers, workstations, network printers, scanners, and other embedded devices with computing power and network connectivity. These devices are usually owned and managed by the organisation and used by employees to perform work functions. This definition excludes Bring Your Own Devices (BYOD).
- 5.15. **USB:** Universal Serial Bus - Is an industry standard that defines the cables, connectors, and communications protocols used in a bus for connection, communication, and power supply between computers and electronic devices.

6. ANSWERS TO FAQ

- 6.1. What Anti-Malware Software is currently in use at CPUT?
Windows Defender.
- 6.2. How can the software be installed on my desktop or laptop?
Anti-malware software is already integrated into the latest available version of Windows in use.
- 6.3. Is the software available for private desktops and laptops?
No, the software is not available for private desktops and laptops.
- 6.4. How do I know that my anti-malware software is up to date?
The anti-malware server sends updates to all computers connected to the Microsoft Active Directory domain daily, keeping all systems up to date. A Windows notification message will alert a user if the definition file is out of date.
- 6.5. Will I have full control over the Anti-Virus settings?
Users do not have full control over the settings., Allowing full control could potentially lead to misuse or compromise the system's overall security and/or integrity.
- 6.6. Is it possible to have contact details or an email address for an administrator to resolve issues when the anti-malware software blocks academically relevant websites?
All IT related incidents must be logged with the CTS Service Desk.

7. EFFECTIVENESS OF THE POLICY

Performance indicators for this policy is listed below:


- 7.1. All university owned computing devices on the network must have anti-malware software installed on them.
- 7.2. All university owned computing devices on the network must have anti-malware definitions that are up to date
- 7.3. Anti-malware monthly compliance reports.
- 7.4. Monthly malware infection reports of incoming and outgoing emails.
- 7.5. Monthly reports showing the version of the anti-malware software and update status on the critical servers and endpoint devices
- 7.6. Reports of periodic malware scans carried out and related results.

8. RESPONSIBILITY

Accountability and Authority:	
Implementation:	<p>The End User Computing (EUC) team within CTS is responsible for determining antivirus requirements, reviewing, approving, installing, configuring, monitoring, and maintaining antivirus software as well as additional technical anti-malware controls on university-owned computing devices.</p> <p>The EUC team within CTS is responsible for ensuring that CPUT users are informed/notified about applicable anti-malware updates available for use on university-owned computing devices.</p> <p>The EUC team within CTS is responsible for developing and maintaining applicable standards and procedures that support this policy.</p> <p>All users are responsible for ensuring that they have up-to-date anti-malware solutions enabled on their devices prior to connecting to the CPUT network.</p>

	<p>The IT Service Desk is responsible for providing first-line support for IT users regarding malware support issues and concerns.</p> <p>Third-Party service providers are responsible for ensuring that all IT systems they provision, whether on-premises or hosted in the Cloud, have suitable anti-malware software installed and configured before connecting to the University network and processing University data assets.</p>
Compliance:	All CPUT users
Monitoring and Evaluation:	Senior Director: CTS, CTS Management
Development/Review:	Senior Director: CTS, CTS Policy Working Group, CTS Management.
Approval Authority:	Council
Interpretation and Advice:	CTS Management

Policy Development Framework				
Policy Type(s):	<p>A: Institutional Governance Policy.</p> <p>B: Administrative Policy.</p>			
Type:	Policy	√	Guideline	Manual
	Procedure		Regulation	Plan
CPUT Statute and/or Regulation Reference no. and date:	Cape Peninsula University of Technology Statute, Government Notice No 46382 of 20 May 2022.			
Relevant Legislation and/or Policy, Codes of practice, Professional authorities:	<ul style="list-style-type: none"> Control Objectives for Information and Related Technologies (COBIT) 2019 National Institute of Standards and Technology (NIST) Cyber Security Framework (CSF) Protection of Personal Information Act (POPIA) No 4 of 2013. 			

Relevant Institutional Policies/ documents/manuals/ handbooks	<ul style="list-style-type: none"> • Information Security Policy • Access Management Policy and Standard • IT Service Management Policy • Electronic Communication Policy • IT Change Management Procedure • Vulnerability Management Procedure • University Institutional Handbooks • Disciplinary Policy. 				
Consultation Process To be verified and signed off before approval	<ul style="list-style-type: none"> • Registrar's Office • CTS Management • CTS Policy Working Group • Newsflash • Business ICT Committee • Management Committee • IT Governance Committee • Council Approval 				
Policy Owner/Sponsor	Deputy Vice-Chancellor: Operations				
Compliance Officers	Senior Director CTS.				
Certification of Due process: To be verified and signed once approved by the relevant authority	 Vice Chancellor 18.01.2024 Date				
Approval Date		Commencement Date		Review Date	

REVISION HISTORY: Only applicable to amended or reviewed Policies. Record details of amendments/revision.					
Version No.	Approved/ Rescinded	Date	Approving Authority	Resolution Number/ (Minute number)	Date for next review (start date for review process)
1.0			Council		

<i>For office use only</i>	
Policy Group (Broad Policy field)	Governance and Administration
Subject (Policy sub-field)	Policies
Reference Number	5/1/P
Version Number	1.0
Key Words:	Policy, Policy template, Policy framework, Policy approval, Policy review