ICTS Policies

UCT ICTS Antivirus Policy

Document summary

Effective date	1 August 2014	**Last updated**	25 July 2014
Policy owner	ICTS		
Approved by	ITMT		

Table of Contents

Purpose

To ensure a computing environment which is free from computer viruses and other malicious code by preventing the infection of computers, networks and technology systems used at the University of Cape Town (UCT).

Applicable to

The policy is applicable to all UCT staff, students, visitors, contractors, partners and collaborators, as well as any other persons engaged in activities at UCT that involve access to UCT computers, networks and/or technology systems.

Policy summary

This policy outlines the responsibilities of ICTS, as well as UCT staff, students and visitors with regards to protecting the integrity and reliability of UCT's network.

Policy details

1. All devices connected to the UCT network or networked resources shall have anti-virus software installed and configured so that the virus definition files are current, routinely and automatically updated.
2. The anti-virus software must be actively running on all computer devices connected to the UCT network or networked resources.
3. All computer devices must be configured such that they schedule regular system and software updates as provided by the respective vendors.
4. All files on computer devices must be regularly scanned.
5. It is the responsibility of all users of the UCT network and networked resources to adhere to this policy and to refrain from any activity that might circumvent this policy.
6. It is expressly prohibited to create and/or distribute malicious code over UCT's network and networked resources.

Anti-virus software

UCT provides Trellix (formerly known as McAfee) anti-virus free of charge to staff and students. UCT staff and students are permitted to use the Trellix anti-virus on their personally owned devices.

Policy violations

1. Computing devices deemed to be infected or posing a threat of propagating computer viruses and/or other malicious code may be disconnected from the UCT network until such time as the infection has been removed and the threat has been fully addressed.
2. Access will only be re-enabled once the device complies with the above requirements and is considered secure and free of malware and is secure. The root cause of the infringement must have been identified and remedial actions must have been taken to prevent a reoccurrence.
3. Any person found to have violated this policy may be subject to disciplinary action.

Policy exclusions

1. Devices that cannot have antivirus software installed on them, for example vendor-managed closed systems, or devices for which antivirus software has not yet been developed.
2. Exceptions to policy for specialised equipment where prior authorisation for the use of such a device was obtained from ICTS.
3. Where an exception has been granted and such a computer device becomes infected then that device will be disconnected until such time as the infection is removed and a solution has been introduced to prevent re-infection.