ICTS Policies

Policy on unsecured computers at UCT

Document summary

Effective date	October 2008	**Last updated**	25 February 2011
Policy owner	ICTS		
Approved by	ITMT		

Table of Contents

Purpose

- Protect the integrity and reliability of the UCT Network.
- Ensure the smooth operation of UCT business conducted via the network.
- Regulate the use of non-UCT computers on the network.

Applicable to

The policy is applicable to all users (staff, students and visitors) of the UCT network.

Exclusions

This policy does not apply to:

- owners of specialised equipment. See: Exceptions to the supported hardware policy.
- operating systems or applications not allowed on the UCT network for security reasons.

Policy summary

This policy outlines the responsibilities of ICTS and the computer user with regards to protecting the integrity and reliability of UCT's network.

Policy details

1. Responsibilities of ICTS

1.1. Protect the UCT Network (and the Internet at large) from individual computers that are unsecured and/or virus-infected.

1.2. Track the actions taken to remedy the problem, via ServiceNow, in order to facilitate re-enabling full network access.

1.3. Inform the computer user of the virus infection or security vulnerability where possible.

In most cases, only the IP address of the computer is known. This information does not allow ICTS to associate a PC with a particular UCT staff member.

1.4. Keep the virus scanner and signatures on UCT servers reasonably current.

Users running supported operating systems will have their virus scanners updated automatically.

2. Responsibilities of the computer user

2.1. Users running supported operating systems must:

2.1.1. ensure that they run the ICTS supported virus scanner on their computer.

2.1.2. run any security patches recommended by ICTS.

2.2. Users running unsupported operating systems must:

2.2.1. ensure that they run suitable virus protection software, and keep it up to date.

2.2.2. ensure that they configure their computers securely.

2.2.3. apply appropriate security patches at regular intervals.

2.3. If a computer is blocked as a result of being a risk to the network, the computer user must contact ICTS to arrange to have the problem fixed and access restored.

Policy violations

1. Access to the UCT network will be revoked if a computer that connects to the network:

1.1. does not have a suitable virus scanner, with the latest virus definitions, installed.

1.2. does not have the appropriate security patches installed.

1.3. is infected with malware that may cause problems on the network or can exploit security vulnerabilities.

2. Access will only be re-enabled once the computer complies with the above and is considered free of malware and is secure.