ICTS Policies

Policy on Network Access from Residence Computers

Document summary

Effective date	4 October 2004	**Last updated**	25 January 2013
Policy owner	Information and Communication Technology Services		
Approved by	ITMT		

Table of Contents

Background

A number of Student Residences are networked providing students living in residence access to information resources, including computer networks and computer equipment. Appropriate use of these computing resources should always be legal and ethical, reflect academic honesty, uphold community standards, and prevent the over consumption of shared resources such as network bandwidth. Appropriate use should demonstrate respect for intellectual property, ownership of data, system security mechanisms, and individual's right to privacy and to freedom from intimidation and harassment.

ICTS and the residences reached agreement on the need for a Policy for Access to the UCT network from Residence computers during May 2003. Given the need for network security and appropriate management of UCT's Internet bandwidth, ICTS implemented a more rigorous firewalling policy for residences.

In order to pursue their academic work, residence students need access to the following services:

- Services on the UCT network (Vula, LinkedIn Learning and departmental web servers)
- Mail
- The web
- FTP

Purpose

This policy allows access to the above services, while restricting access to other services that are not widely required for academic purposes.

Definitions

Term	Definition
UCT network	For the purposes of this document, the UCT network is defined as: *The data network that extends across UCT-owned or -leased premises excluding the Graduate School of Business. The network connects various classes of devices to each other and to third-party networks such as the Internet.* *The UCT network consists of data cables and network infrastructure devices.* Broadly, from the average end-user's perspective, this includes the network up to the plug in the wall.
ResNet	Owner of the content or a section of the content on an official UCT website
Firewall	A security system that controls and restricts both Internet Protocol connectivity and Internet services. Firewalls establish a perimeter where access controls are enforced. Connectivity, as the word is used here, defines which computer systems can exchange information. A service, as the word is used here, is sometimes called an application, and refers to a way for information to flow through a firewall. Examples of services include FTP (file transfer protocol) and HTTP (web browsing).
Perimeter Firewall	The firewall that separates the UCT network from the Internet.

Applicable to

All students who connect to UCT's network from a student residences.

Exceptions

All students and staff that do not connect to UCT's network from a student residence.

Policy summary

This policy outlines the traffic limitations, firewall rules and traffic limit exceptions for students who connect to UCT's network from a student residence.

Policy details

All student residences will connect to the University network from behind routers that will also act as firewalls. These firewalls will be used to manage traffic to and from student residence networks. The following rule sets have been implemented on the firewalls between the UCT network and student residences:

1. Traffic limitations

All traffic limits are bi-directional and apply to both incoming and outgoing traffic from/to the residences.

1.1. All machines on the residence networks run traffic limitations of 128kbit/second per machine.

1.2. These traffic limitations are only in place during office hours (06:00 – 17:30).

1.3. These rules are applied on a per system basis.

2. Firewall rules

2.1. All traffic between residences on the LAN is denied by default.

2.2. Systems on the residence networks are only permitted to initiate connections with machines on the UCT campus network and may not initiate connections with machines external to the campus, with the exception of IRC traffic (port 6667) and the Scifinder scholar servers.

2.3. No connections may be initiated from outside the residences into the residences.

2.4. All mail traffic is diverted to a virus scanning mail gateway.

NOTE:

Apart from the Policy on Network Access from Residence Computers, described here, students must also adhere to the UCT Policy and Rules on Email and Internet Use and Appropriate Use of Computer Facilities Policy. Students must also adhere to all relevant SA laws, regulations, and contractual obligations. The use of UCT's technology resources is a privilege which may be revoked if users fail to comply with these policies.

Policy violations

Students that make use of UCT's network from student residences need to adhere to the above policy and to all relevant SA laws, regulations, and contractual obligations. The use of UCT's technology resources is a privilege which may be revoked if users fail to comply with this policy.