ICTS Policies

Exceptions to the supported hardware policy

Document summary

Effective date	29 October 2009	**Last updated**	4 May 2011
Policy owner	ICTS		
Approved by	ITMT		

Table of Contents

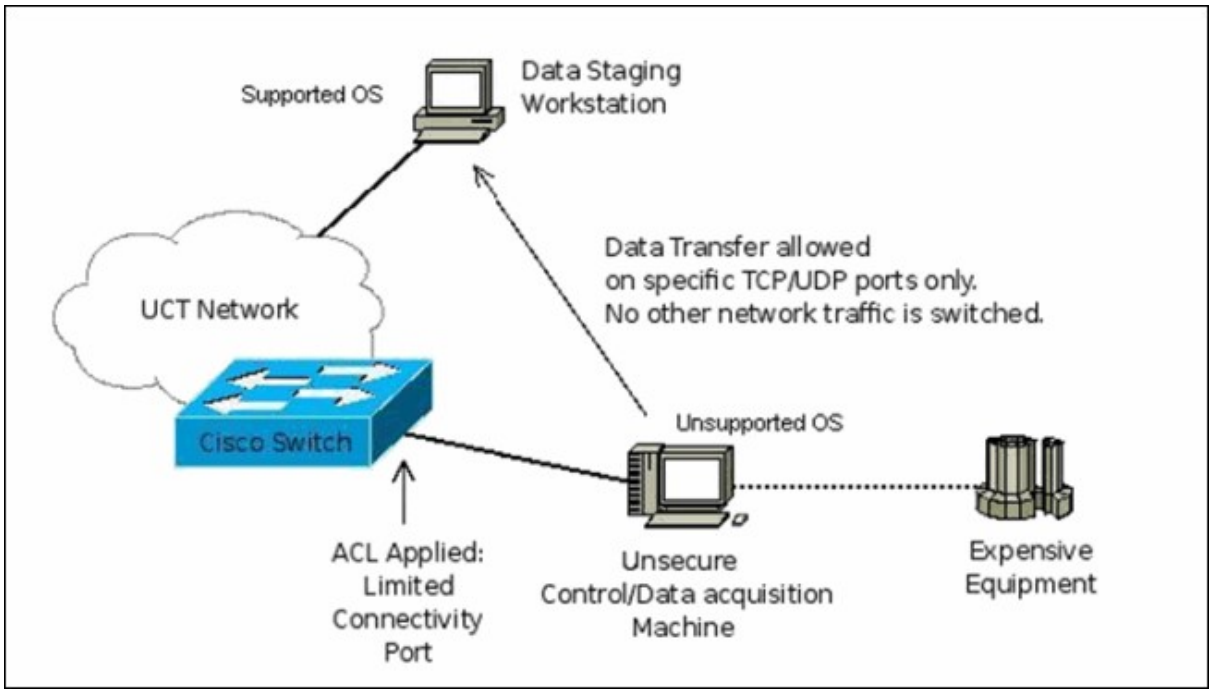
Purpose

Under normal circumstances, old or unsecured computers are removed from the network as they pose a security risk. This document details an exception to this rule.

Policy summary

Old or unsecured computers (unsecured hosts) whose operating systems are no longer secured by the UCT network, and therefore no longer receive antivirus patches, pose a major risk to the network. Because of this, these computers may only have limited access to the network, and only through specialised machines called Data Staging Workstations or "master" computers.

This limited connectivity for unsecured hosts is a short- to medium-term workaround solution allowing these computers to collect data and to transfer such data to a few computers running on one or two specialised machines (see diagram). These computers will not be allowed access to other devices on the network and will only have access to the specialised computers.



Policy details

1. **Under what circumstances will unsecured hosts be allowed to remain on the network**

   1.1. These computers may continue to have access to the network, provided they are:

      1.1.1. Specialised research equipment; and/or

      1.1.2. they are worth more than R500,000.00

   1.2. It is the responsibility of the owner of a computer to ensure that the equipment is up to date and that it enjoys support from the vendor and/or ICTS. Before making purchasing decisions about equipment or software, please check the supported hardware and supported software lists.

   1.3. ICTS understands that specialised equipment plays an important role in the university's core mission of research. Therefore, ICTS envisaged a partnership with owners of such equipment to ensure a greater level of insight into the issues being experienced.

2. **Details of exception**

   2.1. ICTS will consider making an exception to allow unsecured hosts to remain on the network provided that the owner has contacted their vendor and established that an upgrade to a supported operating system is not possible. The workaround that we propose will entail the loss of technical functionality as the older machines will have very limited network access. Owners will have to plan around the limitations. The workaround will allow computers running on unsupported operating systems to collect data from the specialised machines and to transfer such data to one or two computers running an approved operating system. The older machines will only be allowed access to the "master" computer and to no other devices on the UCT network.

This workaround is seen as a short- to medium-term solution. For instance, it is likely that newer technologies adopted in the future may mean that older versions of an operating system will no longer work on the network (e.g. IPv6, 802.1x), as may other currently unforeseen changes to the networking and computing environment. The onus is on the owner of the equipment to ensure that it remains supported.

2.2. Any costs associated with the solution (cabling, switches) are for the account of the owner of the equipment.

2.3. ICTS will not support or assist with any issues on the "data collection" PCs that run operating systems which are out of vendor or community support.

3. Requirements for the data staging workstation and unsecured host

3.1. The data staging workstation:

3.1.1. must run an ICTS-supported operating system,

3.1.2. must have up-to-date operating system patches and anti-virus software at all times,

3.1.3. may not route, bridge or otherwise relay network traffic directly to or from the Unsecured Host (including, but not limited to NAT, VPNs, tunnelling or application layer proxies), and

3.1.4. must use a static IP address allocated by ICTS.

3.2. The unsecured host:

3.2.1. may only communicate with the data staging workstation (on a restricted set of TCP or UDP ports),

3.2.2. may only be connected to one (designated) network point,

3.2.3. will not have access to DNS, DHCP or any other network services,

3.2.4. must use a manually configured static IP address allocated by ICTS, and

3.2.6. the network point must be cabled to the central building distribution/ aggregation switch.