Ulster University Standard Cover Sheet

Document Title	DESKTOP PC PHYSICAL SECURITY STANDARD 2.4
Custodian	Deputy Director of Finance and Information Services (Information Services)
Approving Committee	ISD Committee
Policy approved date	2017 – 08 – 10
Policy effective from date	2017 – 08 – 10
Policy review date	2018 – 08 – 10

Changes to previous version
Page 2 - “with the exception of” changed to “except for”. Page 1 – Remove “Wired network connections once established shall only be changed by technical support staff. Network connections, once established, are tied to specific hardware identification in the desktop personal computer network interface, and switching equipment between network access points can trigger security features disabling the network access point.” Page 1 – Insert “Wired network connections are generally obtained through user authentication via Network Access Control (NAC). Successful authentication allows the device to be tied to the network via the unique Media Access Control (MAC) address. In some circumstances MAC addresses can be changed, but this should not be done. On WiFi connections, a similar process occurs, but the 802.1X protocol is used with Radius servers for authentication.” Page 2 – Insert “A Media Access Control (MAC) address is a unique identifier assigned to network interfaces for communications” Page 2 – Insert “Network Access Control (NAC) is a networking solution that uses a set of protocols to define how to secure access to network nodes by devices when they initially attempt to access the network.” Page 2 – Insert “Radius is a networking protocol that provides centralised authentication, authorisation, and accounting management for users who connect and use a network service.”

INTRODUCTION AND BACKGROUND

Physical security of devices is an important component in assuring the confidentiality, integrity and availability of information.

Further information on ISD policies, standards and guidelines is available at:

http://www.ulster.ac.uk/isd/about-us/policies

RELEVANT LEGISLATION

The University will comply with all legislation and statutory requirements relevant to information and information systems, including:

- Computer Misuse Act 1990;
- Data Protection Act 1998;
- Communications Act 2003;
- Copyright, Designs and Patents Act 1988;
- Freedom of Information Act 2000;
- Human Rights Act 2000;
- Regulation of Investigatory Powers Act 2000;
- Police and Justice Act 2006;
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 ('the Lawful Business Regulations')

POLICY STATEMENT

Desktop personal computers are usually stationary with fixed power supply and network connectivity. Where the network connection is wired, users must arrange through their technical support contact to have their desktop personal computers:

1. Comply with Personal Appliance Testing (PAT) to ensure safe electrical operation.
2. Located and operated in a fashion so as not to pose a health and safety risk and/or possible disruption to mains power supply.
3. Connected to a network access point with either fixed or DHCP IP address availability with reverse lookup table entries where supported for security.

Wired network connections are generally obtained through user authentication via Network Access Control (NAC). Successful authentication allows the device to be tied to the network via the unique Media Access Control (MAC) address. In some circumstances MAC addresses can be changed, but this should not be done. On WiFi connections, a similar process occurs, but the 802.1X protocol is used with Radius servers for authentication.

Desktop personal computers must be switched off outside of working hours, and when not in use for prolonged periods.

When placed in office areas, desktop personal computers must be kept secure with the office locked when necessary. Desktop personal computers in open access areas must only be connected to less privileged wired networks.

All University owned desktop personal computers will be uniquely identified and registered. University owned desktop personal computers are normally assigned to named individuals, except for those in open access areas. Tamper-proof labels must be attached to desktop personal computers for asset identification purposes.

Users shall be aware that when viewing confidential or sensitive information, others may be able to view screen contents. Desktop personal computers must be configured to boot from the local hard disk or network.

PURPOSE AND SCOPE

The purpose of this document is to define University standards for the physical security of fixed location desktop personal computers.

This standard applies to all personal computers connected to the University's data networks owned by the University, and operated by members of the University.

DEFINITIONS AND CLARIFICATION

"PAT Testing" refers to "Portable Appliance Testing" which is a UK system in which electrical appliances are routinely checked for safety. Evidence of testing will be clearly visible to users in the form of "Passed", "Tested for Electrical Safety" and "DO NOT USE after" labels which are affixed.

"DHCP" refers to the "Dynamic Host Configuration Protocol". DHCP is a network protocol used to retrieve IP address assignments and other configuration information.

"IP Address" refers to an" Internet Protocol" address assigned to devices participating in a network as a unique identifier for the purposes of network communication.

"Reverse Lookup Table" refers to record entries in a Domain Name System (DNS) domain that allow translation of a IP Address into a name. This may be used as a security mechanism for network identification.

"Booting" refers to the process that starts operating systems when the user turns on a computer system. The boot sequence is the initial set of operations that the computer performs when power is switched on.

A Media Access Control (MAC) address is a unique identifier assigned to network interfaces for communications

Radius is a networking protocol that provides centralised authentication, authorisation, and accounting management for users who connect and use a network service.