Standard Configuration Details for Computers and other network devices

Owner:	
Approver (Date):	
Review due date:	November 2023
Current Version:	1.1
Update history:	N/A
Document Type:	Operational Policy
Classification:	Internal Only

To discuss receiving the document in an alternative format, please contact University Secretariat.

Document Title

1. Introduction

1.1 The University of Roehampton has a responsibility to uphold the confidentiality, integrity and availability of the data held on its IT systems on and off site which includes systems and services supplied by third parties but managed by the University of Roehampton.

1.2 The University has an obligation to provide appropriate and adequate protection of all its information assets.

1.3 Effective implementation of this policy reduces the likelihood of system compromise by ensuring all devices introduced into the University network have been configured with an agreed baseline.

2. Scope

2.1 All IT systems owned by the University of Roehampton and managed by the University IT department.

3. Responsibilities

3.1 The Chief Information Officer is accountable for ensuring that the policy is adhered to.

3.2 The IT Services Manager is responsible for defining the configuration for all computers and other network devices.

3.3 The University's IT department is responsible for responsible for ensuring that all devices are configured in line with this baseline configuration prior to their issue and for checking that the configuration is still valid when the equipment is returned, or at regular reviews as required.

4. Definitions

4.1 IT Systems refers to:

- Physical Servers
- Virtual Servers
- Cloud hosted Servers
- End user compute devices (laptops/desktops etc.)
- Mobile devices (phones, tablets etc.)
- Network devices
- Operating Systems (both Microsoft and non-Microsoft)
- Applications – (i.e.: Microsoft IIS or SQL etc.)

5. Standard Configuration Settings for Computers and other Network Devices

This document should contain the details of the standard configurations for each make and model of equipment that falls into these categories so that you can be sure that they are returned to this baseline configuration should there be a need.

This work instruction should take the following requirements into account, describing how each is achieved:

- *Removed or disabled of unnecessary built in user accounts*
- *Changed the default password for all user and administrator accounts in line with the requirements in Password Guidance for University Network Accounts*
- *Installation of approved software*
- *Removal or disabling of unnecessary software*
- *Disabled auto-run features (such as those present on removable media) or at least prompting the user to make a choice about what action will occur each time they connect a device.*
- *Enabling of a personal firewall on desktop PCs and laptops, configured to block unapproved connections by default*
- Which systems or information will be accessible via the device