Standard Configuration Details for Computers and other network devices

Owner:	
Approver (Date):	
Review due date:	March 2022
Current Version:	1.1
Update history:	N/A
Document Type:	Operational Document
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 Deputy Director of IT Services is responsible for defining the configuration for all computers and other network devices.

3.3 The University Departments as owners of their business systems and applications are responsible for ensuring any proposed or active system meets the minimum requirements of this policy by timely engagement of IT and IT Security.

3.4 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

All Devices types

- Remove or disable unnecessary built in user accounts
- Change the default password for all user and administrator accounts in line with the requirements in Password Guidance for University Network Accounts
- Install approved software and services only
- Remove or disable unnecessary software and services (Bloat ware, standard services which are not required for the business function of the system)
- Where applicable, to meet compliance or regulations, access from/to devices and resources will restricted as required

On top of the general requirements above, below are additional requirements per type which we are implementing starting with Windows 10 laptops and will progress through to other OS laptops and then other mobiles devices as appropriate

<u>Mobile devices – starting with laptops, future plans for smartphones and tablets</u>

- Enroll on Mobile Device Management
- Install latest OS and security updates
- Enable auto-updates (OS, AV signatures, applications where possible)
- Disable auto-run features (such as those present on removable media)
- Enable local firewall, where applicable, configured to block unapproved connections by default
- Install/verify advanced malware protection
- Enable Remote wipe or lockout via Mobile Device Management for the device, or in case of applications such ones that containing UR Data
- Enforce min. of 6 digit pin for phones and tablets
- Encrypt where necessary

<u>PC and Server</u>

- Install from most current golden image or profile for relevant device/model
- Enroll with Management System(s)
- Disable auto-run features (such as those present on removable media)
- Install/verify advanced malware protection

- Enable local firewall, configured to block unapproved connections by default
- Allow management access only via secure protocols (encrypted transmission of USER/PASSWORD)
    - Where possible and practicle restrict management access to networks of IT support (1/2/3), IT security and management system(s)
- Enable automated upgrades and patching
    - On servers where this is not possible, monitor vendor security notices and vulnerability scans and apply as appropriate

<u>Network devices (switch, access point, router)</u>

- Apply most current common configuration
- Enroll with Management systems
- Configure to restrict management access
    - SNMP access only allowed from
        - management systems (e.g. Cisco Prime) and
        - networks (IT 2/3 and IT Security) and
        - network support partner via VPN
    - Telnet/HTTP disabled
    - SSH v2 or higher with large key size
    - HTTPS

<u>Firewalls and other IT security systems</u>

- Configure to restrict management access
    - SNMP access only allowed from
        - management systems (e.g. Cisco Prime) and
        - networks (IT Security) and
        - security support partner via VPN
    - Telnet/HTTP disabled
    - SSH v2 or higher with large key size
    - HTTPS