User Access Control Policy

Owner:	
Approver (Date):	
Review due date:	March 2022
Current Version:	1.2
Update history:	N/A
Document Type:	Operational Policy
Classification:	Internal Only

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

Contents

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 data compromise due to the misuse (intentional or otherwise) of University of Roehampton network accounts.

2. Scope

2.1 All IT systems owned by the University of Roehampton and managed by the University IT department, including hardware, software, mobile devices, USB storage media, mobile phones and tablets as well as any other peripherals

2.2 This policy applies to all employees, contractors, temporary workers and third parties who use, work with or connect to the University of Roehampton's computer network.

3. Responsibilities

3.1 The Chief Information Officer is accountable for ensuring that the University of Roehampton anti-malware software is installed on all computers connected or able to connect to the University of Roehampton's network

3.2 The IT Services Manager is responsible for ensuring that effective access controls are configured and implemented for all IT systems connected to or able to connect to the University's computer network.

3.3 The IT Services Manager is responsible for ensuring that administrative access to University IT systems is only granted following a formal review and approval process.

4. Definitions

4.1 The University's IT department includes the Core Systems Manager, Solutions Analyst, Deputy Director IT and IT Security Manager.

4.2 IT Systems refers to:

- Physical Servers
- Virtual Servers
- Cloud hosted Servers
- End user compute devices (laptops/desktops etc.)
- Mobile devices (phones, tablets etc.)
- Unstructured file structures/data shares

5. Access Control Policy

5.1 The University of Roehampton controls access to information assets based on business requirements.

5.2 All users of the University's IT Systems will be provided with their own set of unique credentials as part of the University's Account Life Cycle process. The University's disciplinary policy will be invoked in cases of attempted unauthorised access.

5.3 User account requests are subject to UR Account Life Cycle management, including formal authorisation, periodic review and removal. As part of the Account Life Cycle process the departments requesting accounts have to ensure that these accounts will be audited and managed appropriately.

5.4 Users are authenticated to University IT systems at log-on by providing both their username and their password. However in some instances additional means of identification may be required prior to successful authentication.

5.5 Requests for additional access follow a formal approval process and ensure that access is limited to the minimum necessary for the role.

5.6 As part of the University's Account Life Cycle process, user access rights are reviewed when a student/employee/temp/contractors role within the University changes in any way.

5.7 Access rights for all users of the University's IT Systems are reviewed every 12 months and their adequacy is confirmed by the System Owners; any changes that need to take place are actioned in line with the University's User Life Cycle process.

5.8 Requests for Administrator rights to IT systems must be accompanied with a business justification (authorised by Head of Department) and approved by the Deputy Director of IT Services or the relevant system owner. The IT Security Manager needs to be notified about any approved request.

5.9 Where possible Administrator accounts must make use of multi factor authentication when accessing or performing administrative tasks.

5.10 In general Administrator privileges are allocated to a secondary account that has no ability to browse the internet or access e-mail any deviation needs approval by the Deputy Director of IT. These accounts should only be used to carry out functions that need the enhanced rights, with typical day to day activity carried out using their non-administrator account. Therefore where possible and sensible, centralized capabilities may be used to block auto-completing of admin account details on browser-based systems. Where this is not possible, we advise removing these via the steps here.

5.11 Administrator account passwords have to managed in accordance to the Password Guidance for University Network Accounts.

5.12 Accounts with administrator access have to be reported to the IT Security Manager and recorded in the Enhanced Account Register

5.13 Administrator rights are audited in accordance with the University's Account Life Cycle process