Ulster University Policy Cover Sheet

Document Title	User Account and Access Policy 1.4
Custodian	Chief Digital and Information Officer
Approving Committee	Digital and Information Services Directorate
Policy approved date	2021-02-23
Policy effective from date	2021-02-23
Policy review date	2023-02-23

Changes to previous version
Page 1: Change “Unauthorised access to a computer system with intent to commit or facilitate the commission of a **serious crime**” to “Unauthorised access to a computer system with intent to commit or facilitate the commission of a **crime**”. Page 1: Change “Human Rights Act 1998” to “Human Rights Act **2000**”

INTRODUCTION AND BACKGROUND

To achieve its corporate aims and objectives, the University provides staff, students, associates and visitors with user accounts and access to networks, systems and services through assigned roles and entitlements (privileges). This document contains the user account and access policy of the University along with associated information on:

- Related legislation
- Aims, purpose and scope of the policy
- Definition of terminology
- Other relevant policies, standards and guidelines

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

https://www.ulster.ac.uk/isd/it-policies

RELEVANT LEGISLATION

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

- Computer Misuse Act 1990;
- General Data Protection Regulation (GDPR);
- 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

Digital Services Directorate (DS) provides a secure centralised authentication and identity domain for user accounts and access as called for in the University IT Strategy. This authentication and identity domain is the primary and preferred source of authentication and the granting of privileges used by both central and satellite networks, systems and services, and shall be employed whenever and wherever possible.

The centralised authentication and identity domain (currently based around Microsoft's Active Directory) implements both the University Authentication Standard and Password Standard. University networks, systems and services that do not use the centralised authentication and identity domain shall still adhere to these two standards.

User accounts shall be attributed to individuals. Shared user accounts are explicitly disallowed. In certain circumstances, system and process accounts may exist for specific systems management, systems administration and/or engineering purposes. Further specific detail is given in the Authentication Standard.

All user accounts within the University shall adhere to the procedures described in the User Account Management Code of Practice, with particular regard to account creation, management, support and deactivation of user accounts. All user accounts ultimately have a finite lifespan. When users leave the University, their access to University equipment, networks, systems and services shall normally be deactivated. When a user's role within the University changes, their entitlements should also change when/if necessary to the minimum privileges required for their new role.

The following actions are explicitly prohibited by this policy:

- Unauthorised access to computer material (that is, a program or data)
- Unauthorised access to a computer system with intent to commit or facilitate the commission of a crime
- Unauthorised modification of computer material

Remote external access to University networks, systems and services shall only be available through externally exposed web services, or through the following ISD centrally administered methods:

- Secure Remote Access Service (SRAS)
- Remote Access Virtual Private Network (RAVPN)
- Remote Desktop Access (RDA)
- Remote File Share access
- Remote Virtualized Applications (RVA)
- RDweb for browsers

Further detailed information on each of these methods is available in the Remote Access Standard.

In exceptional cases where external access to University servers/services is required, system owners may currently request access using an on-line Server Connection Application Form.

AIMS, PURPOSE AND SCOPE

The aim of this policy is to ensure the confidentiality, integrity and availability of University information resources and to comply with its statutory obligations.

Individual user accounts are established along with entitlements. These are monitored to ensure appropriate use, and user accounts are removed when no longer required. Personal data is protected through these means.

Remote external access to University information is controlled for the purposes of ensuring information confidentiality, integrity and availability.

The scope of this policy is all IT networks, systems and services provided within the University.

DEFINITIONS AND CLARIFICATION

“Internal Information System or Service” is used to refer to any Information System or Service hosted on the University’s telecommunications infrastructure, which is not specifically designed and implemented for public access, irrespective of ownership.

“Remote Access” refers to connections made to the University’s private data communications network and/or an Internal Information System or Service from any computing device which is operated outside the University’s security firewalls and therefore considered not to be connected to a University owned and operated telecommunications infrastructure.

“Secure Remote Access Service (SRAS)” is used to refer to the service implemented and maintained by the Information Services Directorate for the purpose of providing a secure, centrally managed and audited remote access for staff who are authorized to use it.

“Remote Access Virtual Private Network (RAVPN)” refers to a technology which is used to achieve a secure network connection between a Remote User and the University’s private network, over the public Internet. The Remote user may use any mechanism to connect to the Internet in order to initiate the RAVPN to the University, such as a) a home broadband connection via a) an Internet Service Provider, b) a public or private WiFi connection which has access to the Internet, or c) a mobile broadband service from a mobile telephony operator.

“Remote Desktop Access (RDA)” refers to where total control of a personal computer (the desktop), hosted on the University’s private network, is provided to another client computer located on a remote network. Total control means that the remote user is presented with a view of the remote computers desktop and can manipulate the University hosted computer as if they were physically using the University hosted computer on campus.

“Remote Virtualized Applications (RVA)” is the term used to refer to a client computer accessing a pre-defined list of University Applications via a Web based portal. The application is presented in a “window” on the client device, with the application actually running on a University hosted server.

OTHER RELEVANT POLICIES, STANDARDS AND GUIDELINES

- User Account Management Code of Practice
- Authentication Standard
- Remote Access Standard
- Password Standard
- Personal Computer Security Standard
- Networks Standard
- Wireless Networks Standard
- Acceptable Use Code of Practice

CONTACTS AND FURTHER INFORMATION

Contact the ISD Service Desk, email: servicedesk@ulster.ac.uk, telephone: 66777, external: 02890366777.