UNIVERSITY OF HULL

User Management Policy

Classification:	Policy
Version Number:	1-00
Status:	Published
Approved by (Board):	University Leadership Team
Approval Date:	30 January 2018
Effective from:	30 January 2018
Next Review Date:	30 January 2019
Document Authors:	Service Assurance, ICT (D. Chambers, S. Doyle, S. Jones)
Document Owner:	Head of Service Assurance, ICT (Stewart Doyle)
Department/Contact:	help@hull.ac.uk
Summary:	This policy outlines the responsibilities of information risk owners and the principles to be followed to manage user accounts and privileges within related information systems.
Scope:	This policy applies to all University members
Collaborative provision:	Not mandatory
Assessment: (where relevant)	Not applicable
Consultation: (where relevant)	Not applicable
Relevant legal frameworks:	See relevant section of overarching Information Governance and Assurance Policy
Related documents:	Information Governance and Assurance Policy
Published locations:	Public website (www.hull.ac.uk) and SharePoint (share.hull.ac.uk)
Document Communication and Implementation Plan:	Available upon request.

All printed versions of this document are classified as uncontrolled.

A controlled version is available from the university website.

User Management Policy

1. Introduction

1.1. This policy outlines the responsibilities of information risk owners and the principles to be followed to manage user accounts and privileges within related information systems.

1.2. This policy should be read in conjunction with the overarching **Information Security Controls** and **Information Governance and Assurance** policies.

2. Scope

2.1. This policy applies to all information systems managed by, or on behalf of, the University, including those hosted in the cloud.

2.2. This policy applies to all user accounts used to log on to, or interface with such systems.

2.3. This policy applies to all University members responsible for the management of user accounts and the privileges associated to them, specifically those designated as owners or stewards of information systems.

3. Responsibilities

3.1. Information System Owners appointed by the relevant Executive SIRO are expected to understand how access to information is restricted within a given system, which includes how access and privileges are managed.

3.2. Information System Stewards appointed by the relevant Information System Owner have the responsibility for determining how access to information is restricted within a given system, and will usually be responsible for defining how access and privileges within a system should be allocated. They may also be responsible for managing this on a day-to-day basis, or may have the authority to delegate to others.

3.3. Information System Owners/Stewards will work with ICT to produce a clearly defined Access Policy Statement that sets out the rights and privileges of each user (or group of users) within a given system.

3.4. ICT staff who support information systems, known as Service Administrators, may act on behalf of the relevant Information System Owners/Stewards in order to manage accounts and privileges associated to an information system in accordance with an Access Policy Statement and ICT standards.

4. Account Management

4.1. Automatic account creation, deletion and amendment based upon data held in another system, such as the HR or student information system, shall be integrated with the centrally governed and approved University identity management systems.

4.2. All manual management of user accounts including the creation, deletion and amendment must be carried out under the authority of Information System Owners, Stewards, or Service Administrators acting on behalf of owners/stewards.

4.3. Automatic, role-based management of accounts and privileges shall be the preferred approach to user management.

4.4. In the case of ‘service accounts’, the person carrying out account management must be authorised to do so in relation to the specific service.

4.5. An unalterable log should be kept of all account creations, deletions and amendments.

5. Managing Access and Privileges

5.1. Access to systems and the assignment of privileges within those systems should be role based, in that a user should only have access to information and functionality that is required to perform their role effectively.

5.2. Where the technology supports it, user account access and privileges within a system should be linked to centrally held role data, and centrally governed identity management and authentication systems. Exceptions to this should be documented within an Access Policy Statement, and approved by the system owner or relevant executive SIRO. Where exceptions pose a significant risk to information, they may be included in an Information Assurance Risk Register.

5.3. Where user account access and privileges are not being managed as in 5.2, processes will be established and overseen by the Information System Owner/Steward, or suitably authorised individuals to ensure that access and privileges are managed effectively in compliance with this policy.