
Technology & Information Services

EA-ISP-008 User Management Policy

Owner: Nick Sharratt
Author: Paul Ferrier
Date: 28/03/2018 07:36:00

Document Security Level: **PUBLIC**
Document Version: 1.5
Document Ref: EA-ISP-008
Document Link:
Review Date: March 2019

EA-ISP-008 User Management Policy

Document Control							
Version	Author	Position	Details	Date/Time	Approved by	Position	Date/Time
0.90 – 1.3	Paul Ferrier	Enterprise Security Architect	Initial draft created and additional revisions	11/02/2014 – 01/04/2015	Paul Westmore	Interim IT Director	17/02/2015 14:05
1.4	PF	ESA	Reviewed policy	08/09/2017 14:25			
1.5	PW, GB, NS, PF	IT Director, HoSM, 2x ESA	Revised policy before review	06/03/2018 11:25	Paul Westmore	IT Director	06/03/2018 17:20

Introduction

The User Management policy sets out how the user accounts and privileges are created, managed and deleted. It includes how new users are authorised and granted appropriate privileges, as well as how these are reviewed and revoked when necessary, and includes appropriate controls to prevent users obtaining unauthorised privileges or access. It might also include recording of user activity on information systems and networks.

It may be argued that less strict policies than those defined in this document are appropriate for systems that do not store **confidential** or **restricted** information¹. However, it must be remembered that if such systems are connected to the University network they can provide a means of unauthorised access to these categories of information residing in other locations. Whenever possible, therefore, the comprehensive access control regime detailed here should be adopted to mitigate the risks in this area.

1. Access Control

- 1.1 Procedures for the registration and deregistration of users and for managing access to all information systems shall be established to ensure that all users access rights match their authorisations. These procedures shall be implemented only by suitably trained and authorised staff.
- 1.2 Access Control standards must be established for all information systems, at an appropriate level for each system, which minimises information security risks, yet allows the organisation's business activities to be carried out without hindrance.
- 1.3 Where appropriate access to systems will be automatically managed, either indirectly through the use of groups or role based data controls derived from an authoritative source of data (such as the human resources or student records system). Where access is administered manually, changes (especially revocation of permissions) must be performed as soon as possible following notification; it is expected that wherever possible manual processes should be minimised, or replaced where applicable.
- 1.4 A review period will be determined for each information system and control standards will be reviewed regularly at those intervals.

2. Managing Privileges

- 2.1 When automatic management of access permissions and privileges are not appropriate, for example, system administration rights, access must be authorised by the owner of the system and a record must be maintained of such authorisations, including the appropriate access rights and privileges.
- 2.2 System administration must not be performed by the same user account to undertake their normal working operations. Procedures shall be established in order to segregate the risk of compromise to an administrative account.
- 2.3 Procedures shall be established for all information systems to ensure that users' access rights are adjusted appropriately and in a timely manner, whenever there is a change in business need, a user changes their role, or a user leaves the organisation.
- 2.4 User permissions will be allocated on a legitimate business need basis with no access being provided as a minimum.

¹ https://www.plymouth.ac.uk/uploads/production/document/path/6/6015/EIM-POL-001_-_Information_Security_Classification_Policy_v1.1.pdf

3. Password Management

- 3.1 All users shall have a unique identifier (user ID) for their personal and sole user for access to all computing services. The user ID must not be used by anyone else and associated password shall not be shared with any other person for any reason.
- 3.2 Password management procedures shall be put in place to ensure the implementation of the requirement of the Information Security Policy and to assist users in complying with best practice. Documentation is provided in the SEC-GDL-003 University Account Passwords² guidelines.
- 3.3 When working with research data, additional password management requirements, for example shorter timescales for password alteration may be required as part of the research or data sharing contract.

4. Account Management

- 4.1 Documentation of the differing accounts within use around the organisation and their default access levels are to be defined and maintained in the SEC-GDL-004 University Account Access³ document.
- 4.2 Once a unique identifier for an account has been issued, this identifier will not be assigned to any other person at any time within the organisation, this includes the details below:
 - 4.2.1 User ID (the credential to log into an account with, alongside a password, for example, jsmith16).
 - 4.2.2 Email address (for example, john.smith@plymouth.ac.uk)

² [SEC-GDL-003 - University Account Passwords](#)

³ This document is classified as **standard** and therefore is not available for public consumption.