ENTERPRISE
ARCHITECTURE
WITH
PLYMOUTH
UNIVERSITY

Technology & Information Services

EA-ISP-008-User Management Policy

Owner:	Adrian Hollister
Author:	Paul Ferrier
Date:	13/11/2014
Document Security Level:	**PUBLIC**
Document Version:	1.03
Document Ref:	EA-ISP-008
Document Link:	http://blogs.plymouth.ac.uk/strategyandarchitecture/wp-content/uploads/sites/4/2015/04/EA-ISP-008-User-Management.pdf
Review Date:	December 2015

Document Control

Version	Author	Position	Details	Date/Time	Approved by	Position	Date/Time
0.90	Paul Ferrier	Enterprise Security Architect	Initial draft created	11/02/2014	tbc	tbc	Tbc
0.91	Steve Furnell, Paul Dowland	Head of School of Computing, Associate Professor	Alterations and comments provided	04/03/2014 21:50			
0.92	Paul Ferrier	Enterprise Security Architect	Inclusion of no re-use of credentials	11/08/2014			
0.93	Paul Ferrier	Enterprise Security Architect	Updated the document to the new template	13/11/2014 21:50			
0.94	Paul Ferrier	Enterprise Security Architect	Slight tweak to cover default privileges	16/01/2015 14:55			
1.00	PW, AH, GB, CD, PF	Interim IT Director	Approved the policy	17/02/2015 14:05	Paul Westmore	Interim IT Director	17/02/2015 14:05
1.01	PF	ESA	Reworded classification terminology	06/03/2015 14:20			
1.02	PF	ESA	Added reference to Password Guidelines	18/03/2015 15:00			
1.03	PF	ESA	Added 3.3 in reference to research data	01/04/2015 11:30			

EA-ISP-008-User Management Policy

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 **standard** or **restricted** (confidential, sensitive or personal) information. 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, and based on 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 account a user uses 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.

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 Passwords[1] 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 Access[2] 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)

[1] SEC-GDL-003 - University Account Passwords

[2] This document is classified as **standard** and therefore is not available for public consumption.

Appendix

1. Access Control

Explanatory Notes

Access control standards are the rules that an organisation applies in order to control access to its information assets. Such standards should always be appropriate to the organisation's business and security needs. Inappropriate restrictions could result in individual users being unable to do their job, and cause delays and errors in legitimate data processing. Similarly, excessive privilege could allow an authorised use to damage information systems and files, causing delays and errors.

2. Managing Privileges

Explanatory Notes

Good management, including regular reviews, of user access to information systems allows you to implement robust security controls and to identify breaches of access control standards. It is also essential to ensure that the changing role of individuals within the organisation receives commensurate and prompt changes to their access rights.

3. Password Management

Explanatory Notes

Most computer systems are accessed by a combination of user ID and password and, to ensure effective security, they must remain confident and it must not be possible for passwords to be compromised by simple trial and error or by poor management.

4. Account Management

Explanatory Notes

It is extremely important not to re-use account details, it is almost impossible to determine whether an account (albeit user ID or email address) has either been hijacked for use of distributing spam or compromised in some other form and where the details have been published. It is understood with the issuance of more accounts, email addresses become less easy to remember, as with any service provider though, for example, Google[3], Apple[4] and Microsoft etc. re-use of old details must not be undertaken.

[3] https://support.google.com/mail/answer/66278?hl=en

[4] https://discussions.apple.com/thread/5043802?tstart=0