ENTERPRISE ARCHITECTURE WITH PLYMOUTH UNIVERSITY

Technology & Information Services

EA-POL-023 – Password Policy

Author:	Paul Ferrier
Date:	21/10/2016

Document Security Level:	**PUBLIC**
Document Version:	0.91
Document Ref:	EA-POL-023 - Password Policy
Document Link:	<URL>
Review Date:	October 2017

Document Control							
Version	Author	Position	Details	Date/Time	Approved by	Position	Date/Time
0.1	Paul Ferrier	Enterprise Security Architect	Created the document	28/06/2016 13:45			
0.91	PF	ESA	Added account lockout information	21/10/2016 14:15			

EA-POL-023 – Password Policy

Purpose

The purpose of this policy is to establish and enforce practices relating to creation, storage and use of passwords that are required, alongside an appropriate user account to access electronic assets owned and managed by Plymouth University.

Audience

The policy applies to all members and partners of Plymouth University and the equipment that they use to perform their work within the organisation.

Scope

This policy applies to all managed systems, services and interconnected components that afford the IT service provision (irrespective of its physical location) consumed by staff, students and partners at Plymouth University. This policy should also be considered best practice for users' own devices.

Policy

While it is understood that single factor authentication (something you know, for example a password) is prevalent across the organisation, there may be small pockets of two factor authentication (something you know and something you have, such as a security token or biometric) but this is not the norm at present. As such, passwords are integral to the security controls preventing access to materials that need to be protected.

Default passwords

Default administrative accounts and their associated passwords make the management of systems or services *relatively* easy; however, as these credentials are likely to be present on the Internet and accessible to everyone they have no place within our organisation and should be changed at the earliest available opportunity.

Different passwords for different environments

"Systems and services must have different usernames and complex passwords for ***development***, ***test*** and ***live*** environments within the organisation; in this manner if one set of account credentials is compromised it is only that ecosystem that is affected." Extract taken from the EA-POL-022 Access Control Policy.

User passwords

Primarily one set of user credentials should provide access to the majority of (if not all) resources required for day to day business operation. The complexity of these passwords are constrained by the University's Active Directory implementation and any other service that manages cloud based account management, such as Azure Active Directory which is used for Office365. The minimum and maximum password complexity must harmonise these systems to ensure that any given user password will work seamlessly in both environments. Details of the requirements are provided in SEC-GDL-003 University Account Guidelines[1].

In contrast to this though, not all user facing business systems may have the same password requirements, for example financial software may not allow passwords with pound or dollar symbols in them. In this instance it may be preferable to have separate passwords to access these systems for increased security purposes.

Incorrect password lockout

University systems will be protected by an account lockout after six consecutively incorrect attempts. This will slow down any repeated attempts to either guess or try and crack user passwords. This lockout will be in place for half an hour, but can be overridden by Service Desk personnel on request.

Privileged account passwords

Actions that are performed by highly privileged accounts, such as domain, enterprise, system or database administrators (for example) must have, where possible, a password that attains 100% on the CSCAN (Centre for Security, Communications and Network Research) password strength tool[2].

Personal passwords

In an ideal world, every site that requires a combination of username or email address and password should have a different password. This prevents all systems being able to be accessed if your primary account is compromised. To assist in managing the plethora of account credentials it would be worth considering the use of a password manager or vault.

Password storage

Password managers allow credentials to be stored behind a very secure single password (it is the key to your kingdom).

For administrative and operational use, privileged credentials should be stored in an appropriate vault that provides members of staff the ability to perform their required operations without the disclosure of the password. This will then allow the changing of the password on a periodic basis without the need to disseminate a new algorithm to staff.

Auditing

Password changes should be logged for all accounts with details captured covering the date and time, success of the operation, originating computer and/or IP address, to provide a full audit trail of activities.

[1] http://blogs.plymouth.ac.uk/strategyandarchitecture/wp-content/uploads/sites/4/2014/06/SEC-GDL-003-University-Account-Passwords.pdf

[2] https://www.cscan.org/passwordstrength/

EA-POL-023 – Password Policy

Exception Management

Exceptions to this policy may be granted using the Enterprise Architecture Waiver Process and will be considered by the Enterprise Security Architect on merit, risk to University classified confidential or restricted information, as well as alignment with the overall security architecture.

Failure to comply with this policy may lead to the solution architecture being rejected during Enterprise Architecture review, returned for rework or placed on hold. In circumstances where failure to comply leads to a breach of information security or of significant risk of the same, disciplinary action may be taken due to the terms of employment being breached. In addition, any systems configured in a manner that contravenes this policy and other related policies will be disabled pending investigation.

Supporting Documentation

- Enterprise Architecture Principles – Principle 8: Data Security
  - “Security must be designed into data elements from the beginning; it cannot be added later. Systems, data, and technologies must be protected from unauthorised access and manipulation. University’s Executive Group [sic] information must be safeguarded against inadvertent or unauthorised alteration, sabotage, disaster, or disclosure.”
- Information Security Policy – EA-ISP-008 User Management
  - “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.”
- Information Security Policy – EA-ISP-011 System Management Policy
  - “Password management procedures shall be put into place to ensure the implementation of the requirement of the Information Security Policy and to assist users in complying with best practice guidelines.”