Project Management Office
Access Control Policy
Version 2.0
Document: PMO - 1020
Date: 9th February 2017

Access Control Policy

Contents

1. Purpose

1.1.1 The Access Control Policy sets out specific responsibilities, conditions and practices which are designed to address access needs in a manner which minimises risks and maximises the protection of physical assets and sensitive information.

1.1.2 This policy takes into account the requirements of the Data Protection Act and ISO27001:2013

2. Scope

2.1.1 This policy applies to all systems and assets owned, managed or operated by Edinburgh Napier University.

3. Roles and Responsibilities

3.1 HR Role / Line Manager

3.1.1 Inform Information Services of new employees and request access rights.

3.1.2 Inform Information Services of changes to access rights.

3.1.3 Inform Information Services of leavers prior to their departure.

3.1.4 Review access rights and job responsibilities for employees.

3.2 Student and Academic Services

3.2.1 Inform Information Services of new students and request access rights.

3.2.2 Inform Information Services of changes to access rights.

3.2.3 Inform Information Services of leavers prior to their departure.

3.2.4 Review access rights and access to services for all students.

3.3 Systems Managers/Administrators/Owners

3.3.1 Adhere to this policy when executing any changes to access privileges, including positive identification of users requesting password resets.

3.3.2 Review and approve user requests for access to systems.

3.3.3 Audit user and access lists on a quarterly basis to ensure that access is appropriate.

3.3.3 Define and monitor appropriate user groups and roles to support Role-Based Access Control (RBAC).

3.3.2 Maintain systems compliance with legislation, regulation, best practice, internal policies and procedures.

3.3.3 Ensure that all systems enforce the configurations in this policy.

3.4 Information Security Board

3.4.1 Support administrators in defining appropriate user groups and roles to support Role-Based Access Control (RBAC).

3.4.2 Audit user and access lists on a quarterly basis to ensure that access is appropriate.

3.4.3 Perform annual policy and procedure reviews.

4. User Authentication

4.1.1 Each user’s access privileges shall be authorised according to business needs. All privileges must be assigned based on job classification and function. The principle of least privilege must be observed, and evidenced for all access above those systems considered ‘public’. i.e. only the access required to perform a role will be granted. Similarly, access to information will only be granted on a need to know basis. Access control systems must have a default “deny-all” setting.

4.1.2 The use of non-authenticated (e.g. no password) user IDs or user IDs not associated with a single identified user are prohibited. Shared or group user IDs are never permitted.

4.1.3 Every user must use a unique user ID and a personal secret password for access to information systems and networks.

4.1.4 User authentication will be implemented through an automated access control system. Where this is not possible for a given system then access must be managed manually through an alternative set of control procedures.

4.1.5 Edinburgh Napier University must implement authentication procedures of the appropriate strength and manage information security risks to the business. The procedures must be suited for the delivery channel in question. The procedures should be standardised where possible and reviewed periodically by the Information Security Board to confirm secure operation.

4.2 Operating System Access Authentication

4.2.1 Systems must implement a secure mechanism to individually and uniquely authenticate users that access the system remotely or at a local console. Role-based access control will be implemented in line with an access control matrix and authentication must be via password mechanism in line with Active Directory domain policy.

4.3 Web Authentication

4.3.1 Web and other network based applications must implement a secure procedure to authenticate users. Role-based access control will be implemented in the application and authentication will be implemented. Typically this will utilise a password mechanism.

4.4 Voice Authentication

4.4.1 Enquiries for confidential information by telephone must only be disclosed once the identity of the caller has been verified.

4.4.2 IS will aim to ensure that staff are aware of ‘social engineering’ attacks, where the aim is to trick people into revealing passwords or other information that compromises security, and be able to prevent and report such attack attempts to the Information Security Board.

The University will never ask staff or students to supply their passwords.

4.5 Email Authentication

4.5.1 Incoming e-mail to the University must be treated with the utmost care due to its inherent information security risks. The opening of e-mail with file attachments is not permitted unless such attachments have already been scanned for possible viruses or other malicious code. University e-mail is automatically scanned.

4.5.2 Hyper-links in email should only be followed if from a trusted sender.

4.5.3 Care must be taken in answering requests for information via email and the sender's identity confirmed before processing.

4.6 Fax Authentication

4.6.1 Where possible the use of faxes should be avoided. Where faxes are necessary as part of business processes or where faxes request sensitive information or changes to business processes or systems, Information Services must implement a procedure to authenticate incoming faxes which authenticates the sender. This may be a list of approved personnel from the sending organisation.

4.7 White Mail Authentication

4.7.1 Edinburgh Napier University staff must authenticate users who provide written requests for changes to critical business assets or for information by requesting/confirming authentication credentials.

4.8 Network Device Authentication

4.8.1 Any administrative access to network devices must be via an encrypted protocol, e.g. SSH or HTTPS. The exception to this is direct local console access.

5. Access Control Configurations

5.1.1 Passwords must not be shared for any reason.

5.1.2 All users should be assigned a unique ID before gaining access to systems or data.

5.1.3 All first time passwords (including resets) must be set to a unique value per user and changed immediately after first use. Ideally the first password should be system generated and automatically provided to the user. All password reset requests will require the user to identify themselves.

5.1.4 All vendor and default passwords provided with equipment must be changed before a system goes into operation.

5.1.5 Passwords must not be stored in the clear or a reversible hash.

5.1.6 Passwords must be at least 7 characters in length and include the following types of characters:

- At least one Alpha characters
- At least one Number

5.1.7 Reuse of passwords is prohibited. Password history is maintained for at least 24 passwords for staff and 1 password for students.

5.1.8 Password lockout is set to 15 attempts.

5.1.9 Password lock out duration is set to 30 minutes.

5.1.10 Accounts used by vendors for remote access for support services should only be enabled during a pre-defined and authorised change window as needed for the work.

5.1.11 User passwords should be changed at least once annually.

5.1.13 Immediately revoke access for any terminated users.

5.1.14 Verify user identity before performing password resets.

5.1.15 If a password is disclosed, or is suspected of being disclosed, then the System Manager must be notified and the password changed immediately.

5.1.16 Access to databases containing sensitive data should have a separate authentication layer and queries must be restricted to database administrators.

6 Enforcement

6.1.1 Any employee, student or user, found to have violated this policy may be subject to disciplinary or legal action. Disciplinary action may include expulsion for students and the termination of employment for members of staff. Deviation from this policy is permitted only if a valid business case has been provided and subsequently reviewed and approved by the Information Security Board and/or Legal Counsel.