Access Control Policy

Document Status

<table>
<thead>
<tr>
<th>Security Classification</th>
<th>Level 4 - PUBLIC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>1.0</td>
</tr>
<tr>
<td>Status</td>
<td>DRAFT</td>
</tr>
<tr>
<td>Approval</td>
<td></td>
</tr>
<tr>
<td>Life</td>
<td>3 Years</td>
</tr>
<tr>
<td>Review</td>
<td>By June 2012</td>
</tr>
<tr>
<td>Owner</td>
<td>Secure Research Database Analyst</td>
</tr>
<tr>
<td>Retention</td>
<td></td>
</tr>
<tr>
<td>Change History</td>
<td></td>
</tr>
</tbody>
</table>
Contents
Access Control Policy .................................................................................................................. 1
Document Status .......................................................................................................................... 1
1. Introduction ............................................................................................................................ 3
2. Scope ....................................................................................................................................... 3
3. Access Control Principles ........................................................................................................ 3
4. Access Control Authorisation ................................................................................................. 4
5. Access Control Methods .......................................................................................................... 5
6. Access Control Review ........................................................................................................... 5
1. Introduction

1.1 The Institute of Education (IOE) implements Access Control across all its IT systems and services in order to provide authorised, granular and appropriate user access and to ensure appropriate preservation of data Confidentiality, Integrity and Availability in accordance with the Information Security Management Policy.

1.2 Access Control systems are in place to protect the interests of all users of IOE computer systems by providing a safe, secure and readily accessible environment in which to work.

2. Scope

2.1 This policy applies to all IOE networks, IT systems and authorised users.

3. Access Control Principles

3.1 The IOE will provide all employees and other users with the information they need to carry out their responsibilities in as effective and efficient manner as possible.

3.2 Generic or group IDs shall not normally be permitted, but may be granted under exceptional circumstances if sufficient other controls on access are in place.

3.3 The allocation of privilege rights (e.g. local administrator, domain administrator, super-user, root access) shall be restricted and controlled, and authorisation provided jointly by the system owner and IT Services. Technical teams shall guard against issuing privilege rights to entire teams to prevent loss of confidentiality.

3.4 Access rights will be accorded following the principles of least privilege and need to know.

3.5 Every user should attempt to maintain the security of data at its classified level even if technical security mechanisms fail or are absent.

3.6 Users electing to place information on digital media or storage devices or maintaining a separate database must only do so where such an action is in accord with the data’s classification, and are consequently responsible
for ensuring that data security, confidentiality, and integrity are maintained in accord with the Data Security Policy.

3.7 Users are obligated to report instances of non-compliance to the IOE’s Assistant Secretary.

3.8 Instances of non-compliance will be published on IT Services’ risk register and supplied to external auditors upon request.

4. Access Control Authorisation

4.1 Access to IOE IT resources and services will be given through the provision of a unique Active Directory account and complex password. User accounts can only be requested in writing, and by using the appropriate forms, by heads of faculties/departments.

4.2 No access to any IOE IT resources and services will be provided without prior authentication and authorisation of a user’s IOE Windows Active Directory account.

4.3 Password issuing, strength requirements, changing and control will be managed through formal processes. Password issuing will be managed by the Computer Helpdesk. Password length, complexity and expiration times will be controlled through Windows Active Directory Group Policy Objects. Password changing will be performed on IOE workstations or via the remote access Portal.

4.4 Access to Confidential, Restricted and Protected information will be limited to authorised persons whose job responsibilities require it, as determined by the data owner or their designated representative, and as stipulated in the Data Security Policy. Requests for access permission to be granted, changed or revoked must be made in writing.

4.5 Users are expected to become familiar with and abide by IOE policies, standards and guidelines for appropriate and acceptable usage of the networks and systems. All users will have access to expectations, knowledge, and skills related to information security.

4.6 Access for remote users shall be subject to authorization by IT Services and be provided in accordance with the Remote Access Policy and the Information Security Management Policy. No uncontrolled external access shall be permitted to any network device or networked system.
5. Access Control Methods

5.1 Access to data is variously and appropriately controlled according to the data classification levels described in the Information Security Management Policy.

5.2 Access control methods include logon access rights, Windows share and NTFS permissions, user account privileges, server and workstation access rights, firewall permissions, IIS intranet/extranet authentication rights, SQL database rights, isolated networks and other methods as necessary.

6. Access Control Review

6.1 A formal process shall be conducted at regular intervals by system owners and data owners in conjunction with IT Services to review users’ access rights. The review shall be logged and IT Services shall sign off the review to give authority for users’ continued access rights.