Access Control Policy v1.0

University	Oxford Brookes University
Title	Access Control Policy
Creator	Gareth Packham - Head of Information Management
Approvals Required	1. Information Security Working Group 2. CIO 3. Executive Board
Version	Version 1.0
Owner	Chief Information Officer
Subject	The formal, approved, Access Control Policy of Oxford Brookes University
Review date and responsibility	Annually by Head of Information Management.

Revision History

Date	Author	Version Number	Comments
20/09/16	Gareth Packham	0.1 (draft)	Original draft
14/09/16	Gareth Packham	0.2 (draft)	Minor revisions only
19/01/17	Gareth Packham	1.0 (live)	Minor revisions only

1. Policy Objectives

1.1 To define the requirements of Oxford Brookes University (OBU) to ensure that access to information assets is authorised and subject to identification and authentication controls

1.2 To establish the requirements for controlling access to OBU information or information that it is responsible for, including computing and physical resources. Computer systems, networks and allied hardware and other peripherals are an integral part of our operations and represent substantial investment.

1.3 It is the purpose of the Access Control Policy to ensure that all access to information assets is properly authorised, maintained and reviewed.

2. Policy Scope

2.1 This Access Control Policy shall apply to all access to OBU's information assets.

2.2 All Users provided with access to OBU's information systems shall comply with this Access Control Policy as indicated in the IT Acceptable Use Policy.

2.3 Access to physical and non-physical assets will be governed under the same principles.

2.4 This Access Control Policy shall establish the Logical and Physical Access control requirements for protecting the entire university's information systems and hardcopy data.

3. Policy Statement

3.1 This Access Control Policy forms part of Oxford Brookes University’s information Security Management System (ISMS) Framework as defined in the information Security Policy.

3.2 This policy should be read in conjunction with OBU’s IT Acceptable Use Policy, which summarises what OBU deems to be acceptable use of information systems

3.3 It is the responsibility of every User with access to the university's information systems to ensure that they have read and understood this document. All Users are obliged to adhere to this policy. Any deliberate or informed breach of this Policy may lead to disciplinary action up to and including dismissal from the university in accordance with the Acceptable Use Policy.

3.4 OBU’s information systems are provided for business purposes only and this Access Control Policy is used to ensure that Users:

- Comply fully with current legislation;
- Comply with other relevant OBU policies.
- Do not introduce unnecessary risk to OBU.

3.5 Access allocation shall be monitored to ensure compliance with this Access Control Policy.

3.6 All Users, who use the university's information assets and information systems, shall be responsible for safeguarding those resources and the information the information Owners hold, from disruption or destruction.

3.7 The Access Control Policy shall apply to all Users who have access to the university's information assets, including remote access.

3.8 Failure to comply may result in the offending employee being subject to disciplinary action up to and including termination of employment as per the Information Security Policy.

3.9 The use of the university's information assets and information systems indicates acceptance of this Access Control Policy.

4. Implementation Responsibilities

4.1 Oxford Brookes University IT Services shall ensure that Users are provided with education and training to ensure compliance with this Access Control Policy.

4.2 Oxford Brookes University IT Services shall develop, maintain and publish standards, processes, procedures and guidelines to achieve compliance with this Access Control Policy.

4.3 Annually review the Access Control processes, standards and procedures, to achieve compliance with this Access Control Policy and shall support the Access Control Strategy and provide security specific input and guidance where required.

4.4 IT asset owners and authorised users shall be assigned for each identified IT asset in order to approve or reject requests for access to their system.

4.5 IT asset owners and authorised users shall check the validity of all user access requests to information assets owned by them before implementation.

4.6 IT asset owners and authorised users shall authorise employees requiring access to information assets owned by them.

4.7 Human Resources (HR) shall inform the IT department of users starting, moving and leaving the university.

4.8 All appropriate managers shall authorise any requirement to changes to user's access rights on the information systems.

4.9 Users shall not share access codes and/or passwords, if access to other information systems are required then a formal request shall be put forward for authorisation by an appropriate manager.

4.10 Users shall not share their physical access cards; if physical access to restricted areas is required then a formal request shall be put forward for authorisation by the line manager.

4.11 Users shall be responsible for the security (and secrecy) of their own secret authentication information. In no circumstances is secret authentication information to be shared.

4.12 Users shall ensure incidents are reported and escalated in-line with documented Information Security Incident Management Procedure.

4.13 The University shall be responsible for ensuring all Users of OBU's information systems read and acknowledge the policy principles extracted from this Access Control Policy and included in the Acceptable Use Policy.

5. Policy Principles

5.1 All information assets shall be "owned" by a named individual within OBU.

5.2 A process for user access requests, which mandates the steps to be taken when creating or modifying user access shall be defined, documented, annually reviewed and updated. The scope of this process must include network, application and database access and be applicable to any third party access.

5.3 Access to information assets shall be restricted to authorised employees and shall be protected by appropriate physical and logical authentication and authorisation controls.

5.4 Users shall be authenticated to information systems using accounts and passwords. See OBU's Password Policy for further details.

5.5 Users are required to satisfy the necessary personal security criteria, as defined by

OBUs Recruitment Policy, before they can be authorised to access information assets of a corresponding classification.

5.6 Users who have satisfied all necessary criteria may be granted access to information assets only on the basis that they have a specific need to know, or to "have-access-to", those information assets.

5.7 The classification of an information asset does not, in itself, define who is entitled to have access to that information. Access is further filtered by any applicable privacy restrictions as dictated by other OBU Policies (such as the Data Protection Policy)

5.8 Access privileges shall be authorised by the appropriate information Owner and allocated to employee, based on the minimum privileges required to fulfil their job function.

5.9 Administrator accounts shall only be granted to those users who require such access to perform their job function. Administrator accounts shall be strictly controlled and their use shall be logged, monitored and regularly reviewed.

5.10 Users with administrator access shall only access sensitive data if so required in the performance of a specific task.

5.11 Users with administrator access shall also have an unprivileged account, which shall be used for all purposes not requiring administrator access, including but not limited to electronic mail.

5.12 Line managers, information asset owners and authorised users shall ensure rights and privileges granted to Users of information assets are reviewed on at least every 6 months to ensure that they remain appropriate and to compare user functions with recorded accountability. This shall include access to user accounts, which shall be revoked when they have been inactive for more than 90 days.

5.13 Access shall be granted only to those systems or roles that are necessary for the job function of the user. Regular maintenance will address the management of privilege creep.

5.14 Detailed processes shall be developed and followed for terminating, modifying or revoking an employee's access, as part of the Movers/Leavers process.

5.15 In certain instances, particular access may be required for emergency reasons, such as undertaking emergency system maintenance. Requests for emergency access shall be directed to the OBU Chief Information Officer, or a member of the OBIS Executive, and shall be approved by the information asset owner or authorised user. Requests and approval should be documented, if possible, before the change is required stipulating an expiry period, which shall be enforced, for the access rights. A request for change shall be documented retrospectively where it is not possible to do this in advance.

5.16 All third party access (Contractors, Business Partners, Consultants, Vendors) shall be authorised by an appropriate information Owner and, if necessary, monitored.

5.17 Third Party Access to information assets shall be granted in increments according to business need and identified risks. Information asset owners shall specify access timeframes and be prepared to offer justification for such access.

5.18 Remote access to OBU's networks shall be appropriately authorised on a least privilege basis, with access only granted to systems and resources where there is an explicit business requirement. Only employees of the university or authorised third parties shall be able to connect to the university's corporate infrastructure remotely.

5.19 Only authorised personnel shall be given access to secure areas at the university's premises and any third party premises where sensitive information is processed or maintained, or physical assets are held.

5.20 All access to areas hosting systems that store, process, or transmit sensitive data (e.g. datacentres) shall be controlled, monitored by cameras and logged. Logs shall be regularly audited, correlated with other logs and securely stored for at least three months, unless otherwise restricted by law.

5.21 All visitors shall have authorisation prior to entering any of the university's sites where sensitive data is processed or maintained.

5.22 All visits shall be logged and details of logs retained for a minimum of one month, unless otherwise restricted by law. Reception staff shall be made aware of their responsibility to log every visitor to OBU sites.

5.23 Employees shall challenge and/or report any visitors found unsupervised or acting suspiciously at any site where sensitive OBU data is processed or maintained.

5.24 User account names and actions performed shall be recorded using Audit logging capabilities.

5.25 The OBIS Information Management Team shall maintain plans indicating time schedules of all information security access audits to be performed across OBU to ensure compliance with this Access Control Policy.

5.26 Site management shall perform a formal review of physical access rights at least every 6 months to identify unauthorised or expired access. Access controls shall be revoked in instances where access is no longer necessary for job function.