INFORMATION SECURITY POLICY
OF THE UNIVERSITY OF BIRMINGHAM

DOCUMENT CONTROL

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
<th>Authors</th>
</tr>
</thead>
<tbody>
<tr>
<td>18/09/17</td>
<td>Approved by UEB</td>
<td>D. Deighton</td>
</tr>
<tr>
<td>29/06/17</td>
<td>Approved by ISMG with minor changes</td>
<td>D. Deighton</td>
</tr>
<tr>
<td>24/03/17</td>
<td>Annual review – amended for overseas campuses, GDPR and some clarification and rationalisation, some paragraph renumbering.</td>
<td>D. Deighton</td>
</tr>
<tr>
<td>19/09/16</td>
<td>Approved by UEB</td>
<td>D. Deighton</td>
</tr>
<tr>
<td>07/06/16</td>
<td>Approved by ISSG</td>
<td>D. Deighton</td>
</tr>
<tr>
<td>23/02/16</td>
<td>Annual review 2016</td>
<td>D. Deighton</td>
</tr>
<tr>
<td>15/06/15</td>
<td>Approved by UEB</td>
<td>D. Deighton</td>
</tr>
<tr>
<td>12/05/15</td>
<td>Annual review – PCI DSS updates – approved by ISSG</td>
<td>D. Deighton</td>
</tr>
<tr>
<td>18/02/14</td>
<td>Annual review – Asset Disposal, PCI DSS, audit comments.</td>
<td>D. Deighton</td>
</tr>
<tr>
<td>23/04/13</td>
<td>Annual review</td>
<td>D. Deighton</td>
</tr>
<tr>
<td>10/04/12</td>
<td>Revised policy version 1.0 – ISO 27001, NHS IG Toolkit, Data Classification</td>
<td>D. Deighton</td>
</tr>
<tr>
<td>29/10/07</td>
<td>Information Security Policy version 0.52</td>
<td>P. Scott</td>
</tr>
</tbody>
</table>
## CONTENTS

1. Introduction and Scope .................................................................................. 3
2. Objectives ........................................................................................................ 3
3. Roles and Responsibilities ................................................................................ 4
4. Compliance ........................................................................................................ 5
5. Waiver Process .................................................................................................. 5
6. Protection of Confidential Information ............................................................ 5
7. People ............................................................................................................... 6
8. Environmental Controls .................................................................................... 7
9. Operations Management .................................................................................... 7
10. Systems Development and Maintenance ......................................................... 8
11. Business Continuity Management ................................................................... 8
12. Security Incident Management ....................................................................... 8
13. Asset Disposal .................................................................................................. 8

Bibliography ........................................................................................................... 9
Glossary ................................................................................................................... 9
1. **INTRODUCTION AND SCOPE**

1.1. The University is committed to protecting its people, processes and information by deploying controls that minimise the impact of any security incident. This policy is concerned with Information Security including IT security, or cyber security, as well as the security of physical documents, other artefacts and spoken and written communications.

1.2. All members of the University, and others having access to the University’s information resources, are expected to familiarise themselves with this policy and related standards, procedures and guidance. They must understand their obligations and responsibilities to ensure that information is handled appropriately and securely to protect the reputation and interests of the University and avoid placing themselves or the University at risk of prosecution.

1.3. This document titled ‘Information Security Policy’ is a Policy as defined by the University Regulations and all members of the University, and others having access to the University’s computing facilities, communications networks, information or data wherever physically located, are expected to comply.

1.4. Failure to comply with this policy may result in disciplinary action, prosecution or legal proceedings as deemed appropriate by the University.

1.5. This Policy will be regularly reviewed to ensure it remains current and appropriate in the evolving landscape of threats, vulnerabilities and risks, particularly with reference to legislative or regulatory compliance, contractual obligation and emerging technologies.

1.6. This policy applies all types of access to University information resources and is not limited to members of the University or University supplied, or owned, equipment.

1.7. This policy applies to all locations where the University operates and is not limited to any region, country, campus or building.

1.8. In the context of this policy, the term ‘information’ is used in its widest sense to refer to all forms of data and information, including electronic, optical and printed formats as well as textual and audio-visual communications.

2. **OBJECTIVES**

2.1. The core objectives of this Policy, are to:

- **Prevent**, mitigate and protect against the consequences of security incidents, information leaks or breaches.

- **Ensure** that the University stays within the law concerning information and information management and complies with relevant regulations and standards.

- **Increase** awareness and understanding across the University of the need for good information management, and of the direct responsibilities of every member for protecting the data that they handle.

- **Promote** information security practices that enhance the reputation of the University as a trustworthy, open, honest and ethical organisation.
3. **ROLES AND RESPONSIBILITIES**

3.1. The **University Executive Board** (UEB) is responsible for approving this policy on behalf of Council and providing high-level support for information security throughout the University.

3.2. The **Information Security and Management Group (ISMG)** is the University’s oversight committee for information security and information management, responsible for:
   
   i. Directing, evaluating and monitoring information security and information management activities.
   
   ii. Decision making and resolving issues and conflicts of interest.
   
   iii. Conducting annual reviews of this policy with onward transmission to UEB for final approval.
   
   iv. Ensuring clear direction and visible management support for information security.
   
   v. Ensuring that stakeholders are adequately represented.
   
   vi. Approving standards issued under this policy.

3.3. **Heads of College and Professional Services**, are responsible for ensuring communication of, and compliance with, this policy in their respective colleges and departments.

3.4. **Information Asset Owners** are accountable to the University for information assets within their control and are responsible for approving their legitimate and appropriate business use.

3.5. **Individuals** having access to the University’s information, or information under the custodianship of the University, are responsible for:

   i. Complying with this policy.
   
   ii. Maintaining vigilance and reporting security-related incidents and possible breaches of this policy to the IT Service Desk and notifying the Data Protection Officer in cases involving personal data, in accordance with the University’s Data Protection Policy [2].
   
   iii. Completing the Information Security Awareness Training and Data Protection Training provided by the University at least every two years.
   
   iv. Reading and familiarising themselves with this policy and related standards, procedures and guidance that are appropriate to their roles.

3.6. The **Chief Information Security Officer (CISO)** is responsible for:

   i. Defining, operating, monitoring, maintaining and communicating a system for information security management including policies, standards, procedures, guidance, controls and records to ensure the impact and occurrence of information security incidents stays within the University’s risk tolerance levels and that the University complies with relevant laws, regulations and standards.
   
   ii. Advising the University on information security and related topics.
   
   iii. Approving and keeping records of justifiable Security Waivers and exceptions.
   
   iv. Ensuring the effective management and resolution of security-related incidents and forensic investigations concerning breaches, or suspected breaches, of this policy.

3.7. **IT Services**, and other technical staff, are responsible for compliance with this policy of the systems, networks, facilities and services under their control.
4. **COMPLIANCE**

4.1. The University regards any breach of information security as a serious matter that may result in disciplinary action.

4.2. Compliance with this policy should form part of any contract with a third party that may involve access to University networks, computer systems or data.

4.3. Compliance with this policy will be monitored and any failure to comply, unless covered by waivers as described in section 5, will be viewed as a breach of security. Any such event may be the subject of investigation and possible further action in accordance with University procedures.

5. **WAIVER PROCESS**

5.1. In certain circumstances it may not be practical, justifiable or possible for individual members, sections, functions or systems to rigorously adhere to areas of policy. Where there are reasons why a particular control cannot be implemented, a waiver must be requested from the Chief Information Security Officer.

5.2. All waivers will be for the temporary suspension of security controls until a specified end date, when they must be explicitly renewed or will lapse and no longer apply.

6. **PROTECTION OF CONFIDENTIAL INFORMATION**

6.1. Confidential information will be identified based on risk assessments associated with a breach of confidentiality or integrity. In general, information is confidential if it is of limited public availability; is confidential by its very nature; has been provided on the understanding that it is confidential; or its loss or unauthorised disclosure could have one or more of the following consequences:

   i. Financial loss such as the withdrawal of a research grant or donation, a fine by the Information Commissioner, a legal claim for breach of confidence.

   ii. Reputational damage such as adverse publicity, demonstrations, complaints about breaches of privacy.

   iii. Adverse effects on the safety or well-being of members of the University or anyone associated with it. For example, threats to staff or students engaged in sensitive research or harm to benefactors, suppliers, staff or students.

   iv. Cause the University to be in breach of applicable laws, regulations or contractual obligations.

6.2. Personal data that falls within the scope of privacy laws such as the Data Protection Act 1998, the European Union General Data Protection Regulations (GDPR) and successor legislation shall be treated as confidential and managed according to the Data Protection Policy [2].

6.3. Confidential information must be protected at rest and in transit:

   i. Data should be stored in file servers and central databases rather than local hard drives or removable media.

   ii. File, database or disk encryption must be used except where compensating controls can be shown to provide an equivalent level of protection.
iii. Data transfer over data communication networks must be encrypted to University standards.
iv. Email, and other forms of electronic messaging, must be encrypted if technically feasible for sender and receiver.
v. Paper copies and removable media should be clearly marked and kept in locked cabinets with known key holders.

6.4. Confidential information must be accessible only by authorised persons:
   i. The identity of all who access University systems must be verified using an appropriate level of authentication. Where passwords are used, they should conform to University standards and users must follow good security practices in the selection and use of passwords.
   ii. Additional forms or ‘factors’ of authentication should be used where appropriate, based on an assessment of risk.
   iii. Access records should be kept for at least six months to allow for potential investigations and maintain accountability for user actions.

6.5. Remote access to confidential information should be controlled via well-defined access control mechanisms that:
   i. Grant access only to information for which there is a legitimate business need.
   ii. Use secure access control protocols with appropriate levels of encryption and authentication.

6.6. Copying of confidential information should be limited to the minimum number of copies required and, where necessary, records kept of their distribution. The copies should be deleted when no longer needed and hard copies destroyed.

6.7. Procedures must be in place for the secure disposal or destruction of confidential information according to section 13 ‘Asset Disposal’ of this policy. Paper copies should be securely shredded.

6.8. Procedures should be in place for the management of removable media and mobile devices so that they are adequately protected against unauthorised access.

6.9. Confidential information on portable media such as backup tapes must not be taken off-site unless adequate safeguards are in place, including data encryption where technically feasible and good physical security.

6.10. The University will maintain an inventory of its critical and confidential information assets, including those held as custodian on behalf of third parties.

6.11. Information assets, particularly those that are sensitive or confidential, will be protectively marked and handled appropriately by authorised users.

6.12. Operational plans and procedures will be put in place, and appropriate security measures adopted, to protect against the risks using mobile computing, teleworking and communication facilities with sensitive or confidential information.

7. **PEOPLE**

7.1. Controls will be deployed to reduce the risks regarding human error, theft, fraud, nuisance or malicious misuse of facilities.
7.2. Background verification checks, such as references, for all candidates for employment, contractors, and other potential users will be carried out in accordance with relevant laws, regulations and ethics, proportional to the confidentiality of the information to be accessed.

7.3. Access to information assets will be granted, based upon classification, legitimate authorisation and need. Access may be revoked upon change of role, reassignment or termination.

7.4. Information Security Awareness Training and Data Protection Training will be made available for all staff, who should complete the training at least every two years.

8. ENVIRONMENTAL CONTROLS

8.1. Controls will be implemented, as appropriate, to prevent unauthorised access to, interference with, damage to, or removal of information assets, including supporting computing and network equipment and facilities. These may include physical, technical, procedural and environmental measures.

8.2. Access to facilities storing or processing sensitive information will be strictly governed to ensure that protection measures are commensurate with identified security risks.

8.3. Equipment will be protected to reduce the risks from environmental threats and hazards, power interruptions, and other disruptions caused by failures in supporting utilities.

8.4. Equipment will be correctly maintained to ensure its continued availability and integrity.

8.5. Information stored on removable or portable media, including laptops, will be subject to specific assessment and protection techniques.

9. OPERATIONS MANAGEMENT

9.1. Design, build, testing and operating procedures for information processing facilities, systems and networks will be adequately documented and sensitive operational documentation will be stored securely with restricted access.

9.2. Changes to information processing facilities and systems will be subject to formal change control procedures and records kept of all such changes for at least five years.

9.3. Capacity planning and monitoring will be performed to ensure that adequate processing, storage and network capacity are available for current and projected needs, with satisfactory levels of resilience and fault tolerance.

9.4. Systems and information assets will be regularly scanned for vulnerabilities and further security verification such as penetration testing will be performed where necessary.

9.5. Separation of responsibilities and restricted data transfer will be maintained between live and test or development environments.

9.6. Detection, prevention, and recovery controls to protect against malicious code, fraudulent activity or malfunctioning systems will be implemented. Faults and errors will be logged and monitored, and timely corrective action taken.

9.7. Licensed systems will be operated in accordance with the University’s Software Licensing Policy [3].

9.8. Third party service delivery agreements will be implemented, operated, and maintained. Such undertakings will be monitored and periodically audited.
9.9. System clocks will be synchronised securely, under the control of authorised staff.

10. SYSTEMS DEVELOPMENT AND MAINTENANCE

10.1. The security risk of all system deployment and development projects will be assessed, and access to related information assets controlled. This will include all aspects of integration with existing systems.

10.2. Cryptographic techniques will be used, where appropriate, and the associated keying information will be protected.

10.3. All new information systems, major software and infrastructure changes, upgrades and new versions will be subjected to formal security verification including vulnerability scanning, together with penetration testing and other measures as appropriate, before they go live and regularly thereafter.

10.4. New system deployments and significant changes will not be allowed to proceed if they expose the University to unacceptable risks.

11. BUSINESS CONTINUITY MANAGEMENT

11.1. The University will maintain a coordinated approach to the assessment of business continuity requirements across all aspects of the organisation, and the identification of appropriate areas for further action.

11.2. A formal risk assessment exercise will be conducted in accordance with ISO/IEC 27005 to classify each system according to its level of criticality to the University and to determine where business continuity planning is needed.

11.3. Business Continuity Planning will be developed with provision for each system or activity where the need has been established. The nature of the plan and the actions it contains will be commensurate with the criticality of the system or activity to which it relates.

11.4. Each Business Continuity Plan will be periodically reviewed, updated and tested.

12. SECURITY INCIDENT MANAGEMENT

12.1. Procedures will be established and publicised to ensure a quick, effective, and orderly response to information security incidents and security breaches.

12.2. Mechanisms will be put in place to enable the types, volumes, and costs of information security incidents to be quantified and monitored.

12.3. Relevant, authorised staff will be trained in digital evidence collection, retention, and presentation, in accordance with legislative or regulatory obligations.

13. ASSET DISPOSAL

13.1. Information assets such as laptops, desktop computers, servers, disk drives, tablets, smartphones and any other type of media or device that contains data for which the University is responsible as owner, custodian, data controller or data processor must be securely and safely disposed of when no longer required in such a way as to ensure that the data is wiped or destroyed and cannot be recovered or reconstituted.
13.2. Asset disposal includes, but is not limited to, the following:
   
   i. Disposal of unwanted IT equipment.
   ii. Upgrade of office equipment, e.g. photocopier, scanner, printer, fax, telephones) which may have data storage.
   iii. Replacement, due to a fault, of office equipment.
   iv. Replacement of storage devices in any equipment for the purpose of repairing or upgrading them.
   v. Replacement/Upgrade/End of life of a hand-held mobile device provided to staff as part of a University contract.

13.3. Devices and media that cannot be safely wiped must be physically destroyed in a way that ensures the data cannot be recovered or reconstituted.

13.4. All service providers who acquire University data in the course of business must be contractually bound to comply with section 13 ‘Asset Disposal’ of this document; such contracts must provide for regular audits and compliance checks.

13.5. Compliance will be verified periodically and the Information Security and Management Group (ISMG) will approve changes and improvements, as they deem necessary and appropriate.

13.6. IT Services will publish guidance on asset disposal and will provide advice and assistance via the IT Service Desk and Chief Information Security Officer.

BIBLIOGRAPHY
[2]. Data Protection Policy, University of Birmingham
[3]. Software Licensing Policy, University of Birmingham

GLOSSARY

**Cyber security**  
Also known as ‘computer’ or ‘IT’ security, concerns the protection of information in computer systems, files, databases, networks and media.

**Information Asset**  
Any system, device or media that holds data, including computer systems, databases, disks, USB sticks, paper documents, audio-visual recordings etc.

**Information Asset Owner**  
Generally, a senior member of the University held accountable for defined information assets.

**Information Management**  
The curation, organisation and management of all forms of data and information.

**Information Security**  
General term for the protection of information in any form including electronic (see cybersecurity) as well as visual or verbal communications and records.