1. Why is Information Security Important?

The University relies on IT systems and, to a lesser extent, manual procedures for handling and processing the information supporting many of its activities. Information that the University manages needs to be appropriately secured to protect against consequences of breaches of confidentiality, failures of integrity, interruption to availability and failure to comply with legal, statutory or regulatory requirements.

The core principles of information security are confidentiality, integrity and availability and it is vital that we are able to protect these values with regards to University information assets:

- Confidentiality: ensuring that only those individuals who have a valid and authorised reason to access the information can do so;
- Integrity: ensuring that information is not altered, deleted or otherwise modified by individuals or processes unauthorised to do so;
- Availability: ensuring that the information can be accessed when it is required.

2. What is the University Information Security Framework?

There are numerous separate areas of University activities with associated policies, practices, guidance etc. which have a bearing on Information Security. To help navigate and put these into context, Annex A shows how these all interrelate. This set of documents is known as the ‘Information Security Framework’.

The University’s Information Security Framework is intended to:

- Ensure everyone understands the University’s expectations around acceptable use of University information assets and IT facilities;
- Ensure everyone is aware of the different types of information which the University uses and can recognise and manage the associated range of risks and threats;
- Ensure everyone clearly understands their role and responsibilities in respect of information security management;
- Reduce the likelihood of information security breaches and information loss by ensuring information security requirements are understood at all levels of the University;
- Ensure that we are able to meet our statutory, regulatory and contractual obligations and any other agreed standards or approaches in respect of information security.

The Framework also provides the means to articulate and assure the University’s compliance to relevant legislation or other requirements. The University will abide by all UK legislation and relevant legislation of the European Community and any other agreed legal jurisdiction related to the holding and processing of information. In the case of apparent contradiction between the University’s policies and regulations and legislation, the latter takes precedence.
The University will comply with all contractual requirements related to the holding and processing of information, including but not exclusive to:
- JANET Acceptable Use Policy
- The terms and conditions of licences and contracts.
- The terms and conditions of authentication systems, e.g. Athens.

Further guidance on information legislation is provided on the Information Security (www.warwick.ac.uk/gov/informationsecurity) and Legal Services (www.warwick.ac.uk/legalservices) websites.

3. What does the Framework Cover?

The University Information Security Framework applies to the following:

<table>
<thead>
<tr>
<th>All information systems (manual or electronic)</th>
<th>All information</th>
<th>All individuals (referred to as ‘everyone’ hereafter)</th>
</tr>
</thead>
</table>
| • Owned by the University                     | • Information in any format that the University owns or is handling for another organisation | • Staff, students, third parties if  
| • Being used for University business          | • Software owned or licensed by the University | o Managing or using any system identified here  
| • Connected to networks managed by the University |                                           | o Responsible to the University for handling information identified here |

‘All information’ applies to (non-exhaustive list): research data and administrative information; student and staff administrative information; financial information; teaching and learning materials; strategic planning information; commercial information including contracts and information about University resources (space, equipment).

We use the term ‘information assets’ within the Framework to describe a useful or valuable store of information in any format or an information processing system of any type.

Whilst everyone has a role to play in protecting information, some members of our University community will have specific roles and responsibilities for information security and these are set out in section 4 below. These roles will be used consistently throughout the Framework.

The University Information Security Framework works across the full range of information security activities, namely:
- Data Protection
- Freedom of Information
- Corporate Records
- Intellectual Property and Copyright
- Protection of Information against Cyber and Physical Threats

The University also seeks to align the Framework with allied University activities, such as risk management as well as business continuity and emergency planning, and works closely with specialist areas (IT Services, University Library, Research Support Services, for example) to provide a package of cohesive support and instruction to staff, students and partners across these important areas. The University will adopt, where relevant, the principles of recognised international standards, such as ISO 27001.

Mandatory requirements will be indicated within Framework documentation by using ‘will’, ‘shall’ or ‘must’ and recommended or advisory requirements will be indicated by ‘should’, ‘may’ or ‘might’.
4. What are the roles and responsibilities within the Framework?

The University
It is the responsibility of the University senior management to sufficiently resource and
directly implement the Framework. The University is expected to inform the Information
Commissioner’s Office of any significant information security breach relating to personal data
as per the Data Protection Act 1998 and has an obligation to report any significant breaches
pertaining to other types of protected information to the data owner and other relevant
parties. The University recognises that failure to adhere to its legislative, regulatory and
contractual obligations may result in significant financial and legal penalties and reputational
damage.¹

All Individuals with Access to University Information Assets
Everyone granted access to University information assets (e.g. email, teaching and learning
materials, staff/student information, financial information, research information, and the
systems used to process these) has a personal responsibility to ensure that they, and others
who may be responsible to them, are aware of and comply with the Framework. Failure to
adhere to the mandatory requirements of the Framework could result in disciplinary action².

Everyone is responsible for protecting the University’s information assets, systems and IT
infrastructure, and will protect likewise those belonging to third parties but used in the course
of their work at the University. Protection of University or third party information and assets
could be required contractually, legally, ethically or out of respect for other individuals or
organisations.

Everyone will immediately report any observed or suspected security incidents where a
breach of the University’s security policies has occurred, any security weaknesses in, or
threats to, systems or services. The first steps are to inform your Head of Department and
email Informationsecurity@warwick.ac.uk. Further details of the type of information you
should provide when reporting an incident is available at www.warwick.ac.uk/gov/informationsecurity

Heads or Directors of Academic and Administrative Service Departments³
Heads of Departments, with support from the Deputy Registrar’s Office, are accountable for
ensuring that information and information systems within their department are managed and
used in accordance with the Framework. Heads of Departments must ensure that the staff
within their department are aware of their responsibilities when it comes to information
security, have undertaken all appropriate training to be able to carry out their role and are
adhering to the mandatory elements of the Framework.

Additionally, Heads of Departments will be required to participate in ‘health checks’ from
time-to-time to identify and address areas of non-compliance with the mandatory
requirements set out in the Framework. The Institutional Governance Team will work in
partnership with Heads of Departments to undertake the ‘health checks’ and to provide
subsequent additional support to resolve any issues.

¹ The Information Commissioner’s Office can issue a monetary penalty up to £500,000 if it were determined that the University
did not take reasonable steps to secure personal information or acted in such a way as to knowingly put information security at
risk.
² Further information on the University’s staff disciplinary procedure is available on:
http://www2.warwick.ac.uk/services/humanresources/newpolicies/disciplinary/
³ Hereafter referred to as ‘Heads of Departments’
Further information on the University’s student disciplinary procedure is available on:
http://www2.warwick.ac.uk/services/gov/calendar/section2/regulations/disciplinary
Heads of Departments will do the following if there is a suspected breach of information security:

- Find out exactly what has happened and take urgent action to control any resulting damage (direct or indirect) to individuals, reputation etc. – Advice can be sought in the first instance from the Institutional Governance Team (informationsecurity@warwick.ac.uk or ext 50681);
- Ensure that the incident is reported via Informationsecurity@warwick.ac.uk as soon as possible – more information on www.warwick.ac.uk/gov/informationsecurity;
- Participate openly with IT Services and the Deputy Registrar’s Office in any resulting investigation;
- Make the appropriate changes to local practices or seek co-operation from other areas of the University as required to ensure it does not happen again.

Information Custodians

All corporate information assets\(^4\) will have a Custodian and this will be a senior member of staff. An Information Custodian has management responsibility for controlling the production, development, maintenance, use of, access to, retention, security and destruction of a specific information asset or group of assets. For example, the Information Custodian of staff information is the Director of Human Resources. The Information Custodian may delegate the operational responsibility to a named representative but will remain accountable for ensuring these obligations are met. A list of Custodians is available on the Information Security website.

IT and Information System/Application Administrators

Those responsible for the technical support (System) or user (Application) support of information or information systems, for example database and IT systems or application administrators, must ensure the confidentiality, integrity and availability of information and IT assets are protected by proactively managing risk and ensuring systems are managed to industry standard controls. IT Services publish obligations for systems administrators on its website and can advise on appropriate industry standards (ITIL for example).

Deputy Registrar’s Office

The Institutional Governance and Legal Services Teams will ensure that documents forming part of Information Security Framework are kept-up-to date in response to changes in legislation as well as to reflect the changing University information and IT strategy and requirements. The Framework will be available to all staff and students via the web as part of the Information Security website with updates to the Framework being communicated via the intranet or email as appropriate. The Institutional Governance and Legal Services Teams will also provide training and advice to staff in terms of good information security practice and compliance with information legislation, primarily the Data Protection Act 1998 and the Freedom of Information Act 2000.

---

\(^4\) Corporate information assets are those which are managed centrally and used institutionally for the delivery of core teaching, research, administration and commercial functions (student administrative data, staff data for example)
5. How will the Framework be maintained?

The Information Security Framework will be reviewed on the following timescales:

<table>
<thead>
<tr>
<th>What</th>
<th>When</th>
<th>Approved By</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strategic Statement for Information Security</td>
<td>at least every three years</td>
<td>Information Policy and Strategy Committee (IPSC)</td>
</tr>
<tr>
<td>Regulations</td>
<td>at least every three years</td>
<td>Senate and the Council with recommendation of the responsible University committee or body</td>
</tr>
<tr>
<td>Practices/Procedures and Guidance</td>
<td>at least annually</td>
<td>Relevant Senior Officer or Pro-Vice- Chancellor</td>
</tr>
</tbody>
</table>

Urgent requests for updates to any document within the Framework will be processed as quickly as possible, subject to the appropriate consultation and recommendation within the University governance structure.

6. Who are the main contacts for help with Information Security?

<table>
<thead>
<tr>
<th>Area</th>
<th>Contact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information Security</td>
<td>Institutional Governance Team <a href="http://www.warwick.ac.uk/gov/informationsecurity">www.warwick.ac.uk/gov/informationsecurity</a></td>
</tr>
<tr>
<td>“Report an Incident” procedure</td>
<td></td>
</tr>
<tr>
<td>Practical advice on the protection of information</td>
<td></td>
</tr>
<tr>
<td>Training</td>
<td></td>
</tr>
<tr>
<td>Data Protection</td>
<td>Legal Services Team <a href="http://www.warwick.ac.uk/legalservices">www.warwick.ac.uk/legalservices</a></td>
</tr>
<tr>
<td>Freedom of Information</td>
<td></td>
</tr>
<tr>
<td>Copyright</td>
<td></td>
</tr>
<tr>
<td>Intellectual Property – Trademarks or Service Marks</td>
<td></td>
</tr>
<tr>
<td>IT Security (including encryption, incident response, investigations)</td>
<td>IT Security Services (IT Services) <a href="http://www.warwick.ac.uk/its/servicessupport/itss">www.warwick.ac.uk/its/servicessupport/itss</a></td>
</tr>
<tr>
<td>Intellectual Property (not covered above)</td>
<td>Warwick Ventures <a href="http://www.warwick.ac.uk/ventures">www.warwick.ac.uk/ventures</a></td>
</tr>
<tr>
<td>Research Ethics in respect of Data Collection and Management</td>
<td>Research Support Services <a href="http://www.warwick.ac.uk/rss">www.warwick.ac.uk/rss</a></td>
</tr>
<tr>
<td>Research Data Management</td>
<td>Library <a href="http://www.warwick.ac.uk/library">www.warwick.ac.uk/library</a></td>
</tr>
<tr>
<td>Open Access strategy</td>
<td></td>
</tr>
</tbody>
</table>
### Annex A: Map of Documents within the University Information Security Framework

(elements with ❌ fill are in **draft**)

#### Information Security Framework

<table>
<thead>
<tr>
<th>Regulation (Mandatory)</th>
<th>Data Protection</th>
<th>Cyber Threats</th>
<th>Physical Threats</th>
<th>Freedom of Information</th>
<th>Corporate Records</th>
<th>Intellectual Property and Copyright</th>
<th>Allied Activities</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Regulation 31 governing the use of computing facilities</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Policy (Mandatory)</th>
<th>Data Protection Policy</th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Working Practices for Protecting Electronic Information</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Information Classification and Handling Procedure</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Report an Incident Procedure</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>CCTV Manual</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Regulation of Investigatory Powers Act Statement</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| Practices/Procedures (Mandatory or Recommended) |                |               |                  |                        |                   |                                   |                  |
| **Information Security Workbook for Procurement of Software or Services involving UoW Information** |                |               |                  |                        |                   |                                   |                  |
| **Guidance on Use and Selection of Cloud Service Providers** |                |               |                  |                        |                   |                                   |                  |

---

**Strategic Statement for Information Security v1.2 Approved**

**Page 6 of 7**
Document History

20 May 2013  J. Findlay  Created document with comments from Dr Duncan Hine (WMG, Cyber Security specialist), Verification Group members and Head of Service Development (ITS), Senior Assistant Registrar (Governance, Risk and Continuity) and Head of Institutional Governance Services (v1)

30 May 2013  J.Findlay  Incorporated amendments from IPSC and approved for release

2 Sep 2013  J.Findlay  Annex A updated (v1.1)

1 Oct 2013  J.Findlay  Minor change - Updated email address for incident reporting (v1.2)

The official version of this document will be maintained online. Before referring to any printed copies please ensure they are up to date

Next Review
Summer 2016