Information Security Requirements

As a Head of Division, Head of Department or Faculty Board Chair, you are responsible for ensuring that your division, department or faculty adheres to the key areas of University information security policy presented below. To help you understand what is required of you in each area, we have created a simple checklist which tells you what needs to happen for you to meet those responsibilities. For more information and practical guidance visit www.infosec.ox.ac.uk.

Requirements

Management of Information Security

Take overall ownership of information security within your division, department or faculty	☐
Define and document any specific information security requirements for your division, department or faculty	☐
Identify and assign specific roles and responsibilities related to information security within your division, department or faculty	☐
Embed information security into your management framework	☐

Working with Third Parties

Maintain an up-to-date record of all third parties that access, store or process University information on behalf of your division, department or faculty	☐
Ensure that, for all new agreements with third parties, due diligence is exercised around information security and that contractual arrangements are adequate	☐
Ensure that information security arrangements contained in existing agreements are reviewed and are adequate	☐
Monitor the compliance of third parties against your information security requirements and contractual arrangements	☐

Compliance

Implement appropriate technical and procedural arrangements for information security in your division, department or faculty	☐
Perform regular compliance reviews of your division, department or faculty's information security arrangements against University policy	☐
Report on compliance within your division, department or faculty to your Divisional Information Security Working Group and the Joint Information Security Advisory Group	☐

Training and Awareness

Arrange compulsory information security awareness training for staff within your division, department or faculty to ensure they fully understand information security and come to view it as an integral part of their day-to-day work	☐
Include information security awareness training in your divisional, departmental or faculty processes for new joiners	☐
Keep an up-to-date record of who has completed information security awareness training	☐
Repeat information security awareness training for staff on an annual basis	☐

IT Security

Ensure all systems within your division, department or faculty comply with the University's 'baseline' information security standards	☐
Implement additional security controls where confidential data is processed	☐

Information Asset Management

Classify the information assets they are responsible for	☐
Develop appropriate handling rules for these information assets	☐
Ensure that all users are aware of and have confirmed their understanding of the handling rules	☐
Maintain an up-to-date inventory of all asset usage	☐
Monitor compliance against the information handling rules	☐
Review classification and handling rules annually	☐

Incident Management

Ensure local procedures are in place for the management of information security incidents within your division, department or faculty	☐
Ensure compromised systems are isolated	☐
Ensure all security incidents and breaches are reported	☐
Cooperate with the Information Security Team/OxCERT to ensure vulnerabilities are fixed and/or mitigated	☐

Physical and Environmental

Ensure that any IT facilities within your division, department or faculty have appropriate environmental and physical security arrangements in place	☐
Obtain assurances, where third parties have responsibility for hosting or processing University information on your behalf, that appropriate arrangements are in place	☐

Appendix A: Information Security Policy Requirements

If you are a Head of Division, Head of Department or Faculty Board Chair, you are responsible for ensuring that your division, department or faculty adheres to the key areas of University information security policy. Those policy requirements are presented below.

Management of Information Security

It is university policy that:

- **Heads of Division** are responsible for the oversight of information security arrangements for departments or faculties within their division
- **Heads of Department or Faculty Board Chairs** are responsible for the implementation of effective information security within their department or faculty

Working with Third Parties

It is university policy that:

- All relevant information security requirements of the University and your division, department or faculty are covered in agreements with any third-party partners or suppliers
- All third party's compliance again these requirements is monitored

Compliance

It is university policy that:

- Information security controls must be monitored to ensure they are adequate and effective.

Training and awareness

It is university policy that:

- All staff must complete information security awareness training

IT Security

It is university policy that:

- Appropriate information security controls are implemented to protect all IT facilities, technologies and services you use to access, process and store University information

Information Asset Management

It is university policy that:

- Information Asset Owners should be identified for all University information assets;
- Information assets should be handled according to how critical and sensitive they are
- Rules for the acceptable use of information assets should be documented and implemented

Risk Management

It is university policy that:

- Adequately manage information security risk and carry out risk assessments on IT systems and business processes where appropriate. Information security risk assessments should be:
- Carried out on all information systems on a regular basis in order to identify key information risks and determine the controls required to keep those risks within acceptable limits
- Repeated periodically and carried out as required during the operational delivery and maintenance of the University's infrastructure, systems and processes
- Included in the business case for any new ICT system that may be used to store confidential information

Incident Management

It is university policy that you must:

- Report all information security incidents in a timely manner via appropriate management channels
- Isolate information systems which are suspected of being compromised from the network until incidents are resolved and risks sufficiently mitigated
- Investigate and handle information security incidents properly, efficiently and effectively

Physical and Environmental Security

It is university policy that you must:

- Implement appropriate security controls to protect all IT facilities used by your division, department or faculty to host or process University information