University of Bristol

Information Security Policy

Title	Information Security (Overarching)
Reference	ISP-01
Status	Approved
Version	1.3
Date created	December 2012
Last reviewed	November 2021
Next review	November 2022
Classification	Public

Contents

1. Introduction

Information is a vital asset to any organisation and this is especially so in a knowledge driven organisation such as the University of Bristol, where information will relate to learning and teaching, research, administration and management.

This overarching policy document provides an overview of information security and lists a set of policy documents (sub-policies) which, taken together, constitute the Information Security Policy of the University.

These policies are in place to ensure that information is appropriately secured against the adverse effects of failures in confidentiality, integrity, availability and compliance which would otherwise occur.

2. Scope

This policy is concerned with the management and security of the University's information assets and the use of these assets by its members and others who may have been granted permission to process, store or otherwise handle University information on behalf of the University.

The documents in the Information Security Policy set apply to all members of the University and any others who may process information on behalf of the University.

2.1. Definitions

An information asset is defined to be an item or body of information, an information storage system or an information processing system which is of value to the University.

3. Policy

3.1. Structure

The Information Security Policy document set is structured in accordance with the recommendations set out in the "UCISA Information Security Toolkit", which in turn is based on the control guidelines set out in the industry standard ISO 27001.

This top level document lists a set of sub-policy documents which together constitute the Information Security Policy of the University. All of these documents are of equal standing. Although this policy set should be internally consistent, for the removal of any doubt, if any inconsistency is found between this overarching policy and any of the sub policies, this overarching policy will take precedence.

Each of the sub-policy documents only contains high-level descriptions of requirements and principles. They do not, and are not intended to, include detailed descriptions of policy implementation. Such details will, where necessary, be supplied in the form of separate procedural documents and standards which will be referenced from the relevant, individual sub-policy documents.

3.2. Information Security Principles

The University has previously (in its original Information Access and Security Policy, 2002) adopted the following principles, which continue to underpin this policy:

1. Information will be protected in line with all relevant University policies and legislation, notably those relating to data protection, human rights and freedom of information.
2. Each information asset will have a nominated owner who will be assigned responsibility for defining the appropriate uses of the asset and ensuring that appropriate security measures are in place to protect the asset.
3. Information will be made available solely to those who have a legitimate need for access.
4. All information will be classified according to an appropriate level of security.
5. The integrity of information will be maintained.
6. It is the responsibility of all individuals who have been granted access to information to handle it appropriately in accordance with its classification.
7. Information will be protected against unauthorised access.
8. Compliance with the Information Security policy will be enforced.

3.3. Governance

Responsibility for the production, maintenance and communication of this top-level policy document and all sub-policy documents lies with the University's Chief Information Officer.

This top-level policy document has been approved by the University Executive Board. Responsibilities for the approval of all sub-policy documents is delegated to an Information Governance and Security Advisory Board (IGSAB). Before approving any sub-policy, the IGSAB will consult with other groups as appropriate.

Each of the documents constituting the Information Security Policy will be reviewed annually. It is the responsibility of the Chief Information Officer to ensure that these reviews take place. It is also the responsibility of the Chief Information Officer to ensure that the policy set is and remains internally consistent.

Changes or additions to the Information Security Policy may be proposed by any member of staff, via their Head of School or Division, to the Chief Information Officer.

Any substantive changes made to any of the documents in the set will be communicated to all relevant personnel.

3.4. Sub-Policy Document List

Name ID

Business Continuity ISP-02 – Pending publication

Compliance ISP-03

Outsourcing and Third Party Compliance ISP-04

Human Resources ISP-05

Operations ISP-06 – Pending publication

Information Handling ISP-07

User Management ISP-08

Acceptable Use ISP-09

System Planning and Development ISP-10 – Pending publication

System Management ISP-11

Network Management ISP-12

Software Management ISP-13

Mobile and Remote Working ISP-14

Encryption ISP-16

Investigation of Computer Use ISP-18

PCI-DSS Cardholder Data Policy ISP-19