Document Control
Reference: BUL-POL-8.2
Issue No: 4
Issue Date: 01/09/2020
Page: 1 of 6

Information Classification Policy

Brunel University London

An ISO/IEC 27001:2013: *Aligned Document - Implementing Cyber and Information Security Best Practice*

Internal Use Only

Mick Jenkins
Chief Information Security Officer
Dipa Gorsia
Data Protection Officer

Document control

Version history

Version	Author	Date	Comments
0.1	Andrew Clarke	22 Nov 2016	First draft
0.2	Andrew Clarke	21 Dec 2016	Revisions from Information Access Officer
1.0	Andrew Clarke	06 Apr 2017	Approved - Exec
1.1	Andrew Clarke	08 Oct 2019	DPO Amendment:3.4 Special Category Data always UC
1.1	Andrew Clarke	01 Sep 2020	Annual Review

Document Approval

The contents of this document are classified as Protect to Brunel University London (BUL) information classification. Proprietary information presented in this document may not be used without written consent from BUL and remains the exclusive property of BUL unless otherwise agreed to in writing.

Owner: Michael Jenkins	Chief Information Security Officer
Signature: MGJ	Date: 06 Apr 2017
Approver: Pekka Kahkipuro	Chief Information Officer
Signature: PK	Date: 06 Apr 2017
Distribution:	

This document requires the approval from BUL as defined in the ISMS Compliance document.

1.0 About this document

1.1 Purpose of Document

The University generates and holds a wide variety of information that must be protected against unauthorised access, disclosure, modification, or other misuse. Efficient management of such assets is also necessary in order to comply with legal and regulatory obligations such as the Data Protection Act, and to ensure efficient handling of Freedom of Information requests.

Different types of information require different security measures and hence proper classification of information assets is vital to ensuring effective information security and management. This Information Classification Policy is intended to help staff and students to determine what information can be disclosed to external parties, as well as the relative sensitivity of information that should not be disclosed outside of the University without proper authorisation.

This policy, along with the BUL-PROC-8.02 Information Classification guidelines, assists all members of the University to ensure that correct classification and handling methods are applied during their day-to-day activities and information is managed accordingly.

- University information assets should be made available to all those who have a legitimate need to access them;
- The integrity of information must be maintained; information must be accurate, complete, timely and consistent with other related information and events.

Please refer to BUL-GLOS-000 - SyOPs for the glossary of terms, acronyms and their definitions for the suite of BUL ISMS documentations.

1.2 Responsibilities

Table 1 – responsibilities

Title / Role	Description
Asset Owners (as identified by the University)	• Are responsible for determining the classification of their assets • To ensure assets are correctly labelled and for any steps necessary to ensure their correct handling in line with their classification. • Are responsible for appropriate delegation to custodians
Cyber & Information Security Manager	• Is responsible for maintaining the inventory of assets and services together with their classification levels
Systems Manager	• Is responsible for technical labelling mechanisms

All Managers	• Are responsible for providing direction, as appropriate, on mail/postal services, voice mail and voice communication, fax machines, photocopiers, couriers, and sensitive documents for ensuring that these media or information types are handled in line with these requirements
All employees	• Any user of University information assets (including mobile phones, laptops and/or other peripherals) may have specific custodianship responsibilities identified in their user agreements and have a responsibility to adhere to this policy

ISO 27001 - Conformance

This section indicates the University Conformance to ISO27001:2013.

University ISMS Control Number	SOA – Number A8 – Asset management
ISO 27001:2013 Conformance Control	Information Classification Objective A.8.2 - Information Classification

1.3 Scope

This policy applies to:

- All University data held on any medium, including all forms of hard copy and electronic data.
- All University Colleges, Research Institutes, Administrative and Service Departments.
- All contractors, third party suppliers and external stakeholders.

2.0 Classification Policy

2.1 The University classifies information into three levels (University Confidential, Protect and Unclassified):

- University Confidential must identify the individuals, roles, departments or colleges to whom the information is restricted and is available only to those specified and relevant members with authorisation (see BUL-POL-6.1.1 - InfoSec Roles);

  A breach of confidentiality could result in unacceptable damage with very serious and lasting consequences threatening the University or one of its activities.
- Protect is available to any authenticated member of the University. Typically, if this level of information was leaked outside of the University, it could be inappropriate or ill-timed.
- Unclassified: available to any member of the public without restriction. This information, however, should not be placed into the public domain without reason, such as a request or promotional material.

2.2 It is possible that we could receive information that is classified by Government or other institutions as Secret (HMG Information Security Classification April 2014). We do not expect to classify any information generated at the University as secret. It is reserved for information that could impact on National Security, potentially destabilizing the UK or its allies, including information which is subject to the Official Secrets Act 1989. The information handling requirements associated with this level will be dictated by the information owner on each occasion.

2.3 All information held by or on behalf of the University will be categorised according to the Information Classification level (above).

2.4 The information owner will assess the value, sensitivity and the risk of confidentiality breach to their data set. Once the classification has been established any documents containing this information must be systematically marked as such. It is recommended that each department or research group explicitly identifies information owners. This however differs if you are including any Special Category Personal Data. Please refer to the Information Classification Procedure Paragraph 4.2 for further details.

2.5 Any information which is not explicitly marked will be classified as University Confidential, pending classification, by default to avoid data leakage. In the case of disagreement over the classification level to be used, the more secure level should be adopted. Questions about the proper classification of a specific piece of information or a dataset should be addressed to your manager. Where there is a mix of information from different classification levels, the more secure level should be adopted. Information that is sent externally must be marked with its classification level unless already identified and marked as unclassified whereupon no marking is required on the information distributed. All staff have a responsibility for ensuring that any information sent externally, in any format or media, is correctly classified

2.6 All information must be secured to meet the requirements of their respective classification levels (as above). Guidance on the type of security controls that should be implemented is available in the BUL-PROC-08.02 Information Classification.

2.7 The classification must be included in the document footer, which must be manually set to appear on all pages of the document, or on the media on which it is recorded.

2.8 Information received from outside the University that is used within the ISMS scope must be re-classified by its recipient so that, within the University, it complies with this policy.

2.9 The classification of information assets must be reviewed at least once a year by the Asset Owners, and if the classification level can be reduced, it will be. The Asset Owner is responsible for de-classifying information.

2.10 Asset Owners may delegate ownership responsibility to specific individuals, and this delegated responsibility is known as 'custodianship' (and the individuals concerned are known as 'custodians').

2.11 Where a third party will be responsible for handling the information on behalf of the University, the third party shall be required by contract to adhere to this policy prior to the sharing of information.