BETTER DATA WITH PLYMOUTH UNIVERSITY

Plymouth University

EIM-POL-001 - Information Security Classification Policy

Author:	Elena Menendez-Alonso (Data Architect) & Paul Ferrier (Enterprise Security Architect)
Date:	11/01/2016

Security Level:	**PUBLIC**
Status:	Published
Version:	1.1
Reference:	EIM-POL-001
Document Link:	EIM-POL-001 – Information Security Classification Policy v1.1
Review Date:	08/2016

Document Control						
Version	**Contributors**	**Details**	**Date**	**Approved by**	**Position**	**Date**
0.1	EMA	Initial draft	19/03/2014	-	-	-
0.2	EMA, TAG	TAG and EA review: Added information lifecycle and data storage options. Various other minor corrections.	07/04/2014	-	-	-
0.3	EMA, TAG	Additional TAG/EA review. Minor corrections	09/04/2014	-	-	-
0.4	EMA, PF	New level 1 and 2 classification labels: standard (previously 'internal') and restricted (previously 'confidential')	12/08/2014	-	-	-
0.5	EMA	Content moved to standard document template. Renamed 'Information Classification Policy' and standardised terminology (data/information). Other minor corrections	09/01/2015	-	-	-
0.6	TAG, EMA	TAG review Created separate table for technical requirements	14/01/2015	-	-	-
0.7	PW, EMA	Added technical limitations para and mapping to government classifications.	22/01/2015			
0.8	PF, CD, EMA, AH, JG	Updated to include a fourth category ("Confidential") of classification	16/07/2015			
0.9	PF, CD	Final tweaks before Data Quality review	31/07/2015			
0.91	PF	Updated following comments from Dean of Science and Environment	17/08/2015			
0.92	PF, EW	Alteration following comments from DPO and Digital Curator	25/09/2015			
0.95	PF, GR, JL, CD, EMA, JG, MC	Alteration following EU Safe Harbor European Court Ruling and Office365 project comments	14/10/2015			
0.97	PF, EMA	Alteration following DQC feedback	09/12/2015	DQC		
1.0	PF, EMA	Published version	05/01/2016			
1.1	PF, EMA	Removed OneDrive for Business restriction in "storage" section	11/01/2016	UEG		13/01/2016

1. Introduction

1.1 **Purpose:**

The Information Security Classification Policy sets a framework for classifying and handling Plymouth University (PU) information based on its level of sensitivity, and its value to the University.

1.2 **Audience:**

This policy applies to all members of the University and its partner organisations that have responsibility for any aspect of information creation, collection, dissemination, maintenance, disposal or consumption.

Failure to comply with this policy may result in action under the University's Human Resources policies.

1.3 **Scope:**

This policy applies to all University information and to any activity resulting on the creation, collection, dissemination, maintenance, disposal or consumption of such information through its lifecycle.

1.4 **Limitations:**

It is recognised that, at the time of writing, some of the technical requirements specified in the policy cannot be met (e.g., those around encryption and back-up of 'restricted' data). Nonetheless, the requirements should be adhered to as closely as possible. The policy will inform decision making whenever systems and processes are reviewed or replaced.

Exceptions to this policy should only be made when there are significant reasons that prevent it from being adhered to and they must be recorded by the Enterprise Architect or delegate, through the Enterprise Architecture Waiver Procedure, must only be for a defined period of time and may be reviewed once expired by the Enterprise Architect or delegate.

2. Definitions

Audit	An independent examination of practice to determine its compliance with a set of requirements. An audit may be carried out by internal or external groups.
Availability	Preserving timely and reliable access to information
Confidentiality	Protecting personal and proprietary information from unauthorised disclosure
Data and Information	'Data' are facts and statistics collected together for reference or analysis[1]. When data is processed, organised, structured or presented in a way that gives it context and therefore makes it more useful, it is called 'information'. In the context of this document and the University's Information Governance framework, the terms 'data' and 'information' can be used interchangeably.
EU Safe Harbor	Was a streamlined process that US companies use to comply with EU Directive 94/46/EC on the protection of personal data. ***This is no longer valid as of 07/10/2015.***
Information Asset	Information which is valuable to the University and is managed with the expectation that it will provide future benefit.

[1] Oxford Dictionaries online, 2014: http://www.oxforddictionaries.com/definition/english/data. Accessed: 2014-11-20.

Information Asset Owner	Individuals or group of people who have been officially designated as accountable for specific information assets and for ensuring that procedures have been put in place to maintain and improve standards of data quality and to ensure that the Information is managed securely and in compliance with University regulations and statutory obligations.
Integrity	Preserving the authenticity, accuracy and completeness of information against unauthorised modification or destruction
Lifecycle Management	The process of managing information through its lifecycle (see Figure 1)
Private Cloud	The cloud infrastructure is provisioned for exclusive use by a single organisation comprising multiple consumers (e.g., business units); it delivers the agility, scalability and efficiency of the public cloud, but in addition provides greater levels of control and security. It may be owned, managed, and operated by the organisation, a third party, or some combination of them, and it may exist on or off premise.[2]
Public Cloud	The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organisation, or some combination of them. It exists on the premises of the cloud provider. [2]
Sensitive Information	Information that is private, personal, or proprietary and must be protected from unauthorised access

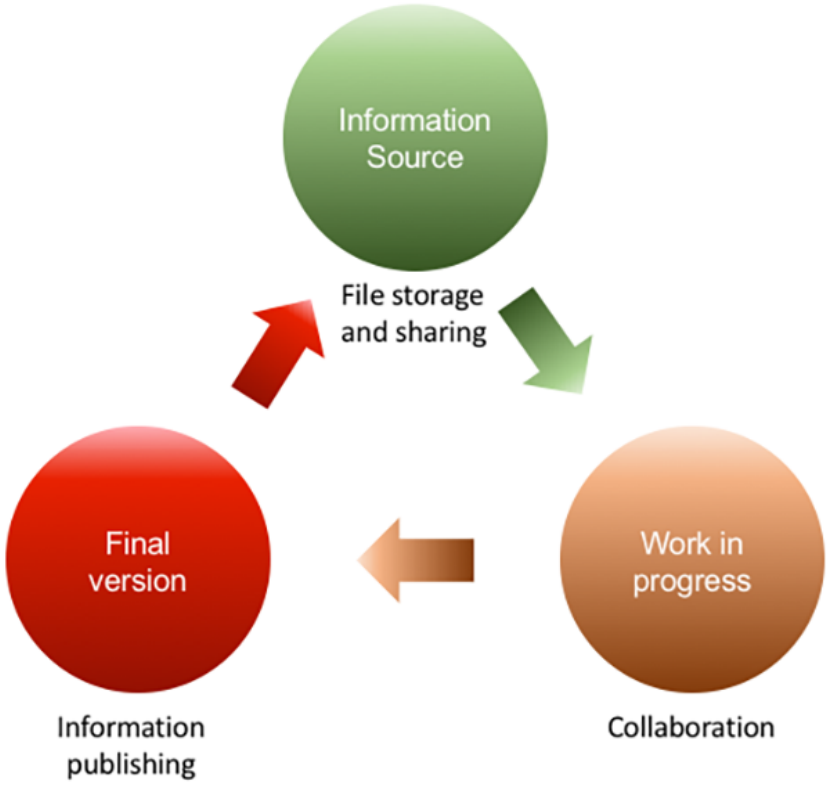

Figure 1. Information lifecycle

File storage and sharing	Content is mainly static, though it may move quickly to the next stage to support collaboration.

[2] Definition taken from NIST Special Publication 800-145 (The NIST Definition of Cloud Computing, September 2011) http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

Collaboration	This is the work in progress, the draft content; once ready to present this is where the approval process resides.
Information publishing	This is the final version of the content. It is official and published for the relevant audience to consume. It is anticipated as much information is made publically available as possible.

3. Assigning classification levels

3.1 The classification of information is based on its level of sensitivity and the impact to the University (e.g.: impact to organisational operations, organisational assets, or individuals) if the confidentiality, integrity or availability of the information is compromised.

3.2 Table 1 outlines the relationship between the level of damage, the security impact and the information security classification level.

Table 1. Relationship between the level of damage, security impact and information classification level

Damage level	Security impact	Information classification
Minimal	Low	Public – Level 4
Moderate	Moderate	Standard – Level 3
Serious	High	Confidential - Level 2
Severe to catastrophic	Extreme	Restricted – Level 1

4. Information security classification levels

4.1 Table 2 lists the information security classification levels across various stages of the lifecycle.

Table 2. Information security classification levels

	Public – Level 4	Standard – Level 3	Confidential – Level 2	Restricted – Level 1
Security impact	Negligible to low	Moderate	High	Extreme
Description	Information should be classified as **Public** when the unauthorised disclosure, alteration or destruction of that information would result in little or no risk to the University and its affiliates (inconvenient but not debilitating). The University has adopted and abides by the **model publication scheme** issued by the Information Commissioner's Office. This means that the University commits to making a significant amount of its information publically available[3].	Information should be classified as **Standard** when the unauthorised disclosure, alteration or destruction of that information could result in a moderate level of risk to the University or its affiliates. A reasonable level of security controls should be applied to Standard information.	Information should be classified as **Confidential** when unauthorised disclosure, alteration or destruction could result in either personal (or sensitive personal)[4] or internal service configuration data being divulged; this equates to the University being at risk from Information Commissioner's Office sanctions and should be considered as a high risk. A significant level of security controls should be applied to Confidential information.	Information should be classified as **Restricted** when the unauthorised disclosure, alteration or destruction of that information could cause an extreme level of risk to the University or its affiliates. The highest level of security controls should be applied.
Examples May include, but not limited to	Programme and course information Press releases Research publications and research datasets cleared for publication Approved University operating policies, e.g. Teaching & Learning, University Services and governance information	Internal documents Collaborative documents of a non-confidential nature Building plans and information about the University's infrastructure	Payroll Student grades Home address Disability information Emergency contact details Notes relating to disciplinary processes Research data containing personal information or information which is of a high value	Commercially sensitive business operations and strategies Medical (including tissue) or Clinical trial research data Any other research data stipulated through the research contract or agreement to be handled with utmost care Account passwords that can be used to access confidential information

[3] For further details, please see http://www.plymouth.ac.uk/your-university/governance/information-governance/publication-scheme

[4] Personal details include anything that can provide reasonable deduction about who the data belongs to – i.e. forename and surname or postcode (specifically in remote locations)

	Public – Level 4	Standard – Level 3	Confidential – Level 2	Restricted – Level 1
Access control	**Viewing:**	Access controls must be observed from creation to destruction. **Viewing:**	Access controls must be enforced from creation to destruction. **Viewing:**	Tight access controls must be enforced from creation to destruction. **Viewing:**
	Unrestricted.	Limited to members of the University, partner organisations and individuals. Not intended for the general public. Information may have limited access for a specific subset of members. Access to information must be requested from, and authorised by, the Information Asset Owner (or their delegate) who is responsible for the asset. Access may be authorised to groups of persons by their job classification or responsibilities (role based access), and may also be constrained by one's department.	Limited to members of the University, partner organisations (where covered by data sharing agreements) and individuals, as authorised by Information Asset Owners (or their delegate). Cannot be disclosed to the general public. Information should have limited access for a specific subset of members. Access should be authorised to groups of persons by their job classification or responsibilities (role based access), and should also be constrained by one's department.	Access must be individually requested and will be granted by the Information Asset Owner responsible for the asset (or their delegate), only to those persons affiliated with the University who require such access in order to perform their job ('need-to-know'). Must not be disclosed to the general public. Where feasible access should be authorised to individual persons, as opposed to groups, if this is not feasible then small groups with appropriate business need should be permitted.
	Printing and copying:	**Printing and copying:**	**Printing and copying:**	**Printing and copying:**
	Unrestricted.	Limited. Printing and copying will be permitted, unless stated otherwise.	Limited. Printing and copying may be permitted, unless stated otherwise.	Highly limited. Authorisation by Information Asset Owner (or their delegate) required and available only to individuals which require access in order to perform their duties.
	Modification:	**Modification:**	**Modification:**	**Modification:**
	Unrestricted, although moderation is advised.	Limited. Authorisation for modification by Information Asset Owner (or their delegate) required.	Limited. Authorisation for modification by Information Asset Owner (or their delegate) required.	Highly limited. Modification should only be performed by Information Asset Owner (or their delegate).

	Public – Level 4	Standard – Level 3	Confidential – Level 2	Restricted – Level 1
Storage	**Electronic:**	**Electronic:**	**Electronic:**	**Electronic:**
	No restrictions.	Working copies of documents can reside on an individual's workstation or a mobile device (e.g. a laptop computer). Device encryption is suggested.	Working copies of documents can reside on an individual's workstation or a mobile device (e.g. a laptop computer). The device should be encrypted using whole-disk encryption. Final or approved copies of documents must be stored within a Document Management System or a shared storage area with appropriate permissions added to prevent unauthorised access.	
	Can be stored in any public cloud, including personal and corporate accounts (for example, DropBox, Google Drive or One Drive).	Can not be stored in any personal public cloud account.		
		Can be stored in the University's public cloud (i.e. Plymouth University Office 365 environment), including One Drive for Business. Can be shared with partners without the requirement for a non disclosure agreement.	Can be stored in the University's public cloud (i.e. Plymouth University Office 365 environment), with restrictions on who can access the materials. **Cannot be shared publically.** Can be shared with partners with a Non Disclosure Agreement being in place between the two parties. Sharing permissions must be controlled by the Information Asset Owner.	Can be stored in the University's public cloud (i.e. Plymouth University Office 365 environment); where not contravening any license or contractual arrangements, with restrictions on who can access the materials. **Cannot be shared publically.** Can be shared with strategic partners but a Non Disclosure Agreement must be in place between all of the relevant parties. Sharing permissions must be controlled by the Information Asset Owner.
	Paper/hard copy:	**Paper/hard copy:**	**Paper/hard copy:**	**Paper/hard copy:**
	No restrictions.	No restrictions.	Do not leave unattended where others may see it; store in a secure location	Do not leave unattended where others may see it; store in a secure location

<table>
<tr><th></th><th>Public – Level 4</th><th>Standard – Level 3</th><th>Confidential – Level 2</th><th>Restricted – Level 1</th></tr>
<tr><td rowspan="2">Transmission and collaboration</td><td rowspan="2">No restrictions.</td><td rowspan="2">Document or File encryption suggested.
Any distributed documents (electronic or paper) should include ‘STANDARD’ in the document header, aligned to the right of the page.
Hard printed copy can be transmitted through the normal mail channels.</td><td>Document or File encryption required for electronic transmission (for example, via email or secure file transfer protocols).
Any distributed documents (electronic or paper) must be watermarked as ‘CONFIDENTIAL’ and the intended recipients clearly indicated; if watermarking is not possible ‘CONFIDENTIAL’ must be included in the document header, aligned to the right of the page.
Printed copies to be delivered in sealed envelopes marked ‘Personal’ or ’Confidential’.</td><td>Document or File encryption required for electronic transmission (for example, via email or secure file transfer protocols).
Any distributed documents (electronic or paper) must be watermarked as ‘RESTRICTED’ and the intended recipients clearly indicated; if watermarking is not possible ‘RESTRICTED’ must be included in the document header, aligned to the right of the page.
Printed copies to be delivered in sealed envelopes marked ‘Personal’ or ‘Restricted’.</td></tr>
<tr><td colspan="2">For collaboration with external parties a non-disclosure agreement (NDA) is required.
A Security Risk Assessment[5] should be performed and approved prior to first use, or after any significant change to the existing service.</td></tr>
<tr><td>Retention</td><td colspan="4">All information must be retained for the legally or contractually required minimum and maximum periods of time[6]. This will vary depending on the type of information under consideration. It is very important that if you unsure of the retention period, please refer to the University’s Records Retention Schedule.</td></tr>
</table>

[5] Please refer to Section 6 - Security Risk Assessment, Exemption process and Authorisation

[6] Data Protection Act – Principe 5 – Retaining Personal Data and Principle 4 – Data Accuracy may apply directly here

	Public – Level 4	Standard – Level 3	Confidential – Level 2	Restricted – Level 1
Disposal	**Electronic**	**Electronic**	**Electronic**	**Electronic**
	No special requirements other than compliance with Retention Schedule (see above).	No special requirements other than compliance with Retention Schedule (see above).	Must comply with Retention Schedule (see above). On decommissioning of equipment used to store the information, the storage must be securely wiped to CESG Enhanced standard[7], or physically destroyed. An accompanying certificate of destruction is required to be obtain by the person facilitating the destruction; the certificate must be stored securely by the Enterprise Security Architect.	Must comply with Retention Schedule (see above). On decommissioning of equipment used to store the information, the storage must be securely wiped to CESG Enhanced standard[7], or physically destroyed. An accompanying certificate of destruction is required to be obtain by the person facilitating the destruction; the certificate must be stored securely by the Enterprise Security Architect.
	Paper/hard copy	**Paper/hard copy**	**Paper/hard copy**	**Paper/hard copy**
	Printed copies can be recycled in the green bags provided around the campus.	Printed copies can be recycled in the green bags provided around the campus.	Printed copies should be cross-cut shred to DIN 66399[8] P-3 standard and disposed of in confidential waste (blue) bags.	Printed copies must be cross-cut shred to DIN 66399[8] P-4 or P-5 standard and then disposed of in confidential waste (blue) bags.
Training	General data protection and information security awareness training mandatory.			
		Refresher training carried out yearly.		
			Applicable policy and regulation training required.	Applicable policy and regulation training required.
User devices	Password protection suggested; locked when not in use.	Password protection required, locked when not in use. Encryption suggested.	Password protection required, locked when not in use. Encryption required.	Password protected required, locked when not in use Encryption required.

[7] CESG Enhanced standard - UK Communications Electronics Security Group (CESG) Enhanced standards

[8] DIN 66399 is the European Security Standard for the Shredding or Destruction of all types of Data Media, as of September 2012

4.2 Table 3 outlines technical requirements associated with the information classification levels.

Table 3. Information classification levels – technical requirements

	Public – Level 4	Standard – Level 3	Confidential – Level 2	Restricted – Level 1
Storage (technical)[9]	Storage on a secure server recommended. Storage in a secure Data Centre recommended. Encryption not required.	Storage on a secure server required. Storage in a secure Data Centre required. Encryption optional.	Storage on a secure server required. Storage in secure Data Centre required. Encryption required.	Storage on a secure server required. Storage in secure Data Centre required. Encryption required.
Backup and disaster recovery	Backups suggested where appropriate.	Backups required where appropriate.	Encrypted backups required where appropriate, with PU holding the encryption keys. Off-site storage in a secure[10] location required.	Encrypted backups required, with PU holding the encryption keys. Off-site storage in a secure[10] location required.
	Backup frequency commensurate with requirements to restore service in service level agreement.			
Network security	May reside on an open public network.	Should not reside on an open public network.	Must not reside on an open public network.	Must not reside on an open public network.
	Protection with a network firewall required, with the rule set reviewed at least quarterly, or after any significant business change or incident.			
		Additional network security measures (for example intrusion prevention or intrusion detection) available based on system or service requirements.		
System security	Must follow general best practices for system management and security. Host-based software firewall suggested.	Must follow University-specific and OS-specific best practices for system management and security. Additional system security measures (for example software firewall, file integrity monitoring) available based on system or service requirements.		
Virtual environments	May be hosted in a virtual server environment. All other security controls apply to both the host and the guest virtual machines.			
			Data should be logically separated (at a minimum) from other classifications of information.	Data must be logically separated (at a minimum) from other classifications of information.

[9] See also EA-POL-014 – Enterprise Architecture Policy – Hosting

[10] Please refer to section 5 - Location restrictions for storage and transmission.

	Public – Level 4	Standard – Level 3	Confidential – Level 2	Restricted – Level 1
Remote access	No restrictions.	Access restricted to local network or Plymouth University's wireless service for on premise resources.	Access restricted to local network or Plymouth University's wireless service using a secure VPN service for on premise resources.	Access restricted to local network or Plymouth University's wireless service using a secure VPN service for on premise resources. Two-factor authentication recommended.
		Access to cloud resources restricted to authorised parties using secure protocols over the Internet. Remote access for 3rd parties restricted to temporary authenticated via secure protocols over the Internet.		
			Unsupervised 3rd party remote access is not allowed. Remote access for University personnel may be limited based on any contractual obligations surrounding research data.	
Auditing	Not required.	Logins, successful and failed attempts.	Logins, successful and failed attempts, access, modifications and permission changes.	Logins, successful and failed attempts, access, modifications and permission changes.

5. Location restrictions for storage and transmission

5.1 In line with data protection legislation, personal information should not be transferred to countries or territories outside the European Economic Area (EEA). The ICO provides advice to help organisations decide whether their storage solutions meet data protection requirements[11].

5.2 Table 4 shows how classification levels affect the choice of storage location.

Table 4. Storage options

	Public (L4)	Standard (L3)	Confidential (L2)	Restricted (L1)
On-site	✔	✔ 🔒	✔ 🔒 ⛊	✔ 🔒 ⛊
Off-site (UK only)	✔	✔ 🔒	✔ 🔒 ⛊	✔ 🔒 ⛊
Off-site (EEA only)	✔	✔ 🔒	✔ 🔒 ⛊	ⓘ 🔒 ⛊ 12
Off-site (Non-EEA)	✔	ⓘ 🔒	ⓘ 🔒 ⛊ 12	ⓘ 🔒 ⛊ 12

Key: ✔ Suitable ⓘ Additional checks required 🔒 Network password protected ⛊ Encrypted[12]

6. Security Risk Assessment, Exemption process and Authorisation

6.1 Where projects, elements of service or research requirements are not able to accommodate the data classification levels stated previously, a security risk assessment must be performed by the Enterprise Security Architect or delegate.

6.2 The risk assessment rankings are provided below:

Risk Rating	Low	Medium	High
Sign Off	Enterprise Security Architect	Strategy & Architecture Manager	IT Director or Chief Information Officer

6.3 The security risk assessment will feed into the Enterprise Architecture Waiver Process, highlighting how any identified risks are to be accepted, reduced or transferred, but not avoided for a designated period of time.

7. Related documents and further information

- Information Governance Roles & Responsibilities
- EIM-POL-002-Data Quality Policy

[11] http://ico.org.uk/for_organisations/data_protection/the_guide/principle_8

[12] Meets PU encryption key management requirements

- EIM-POL-003-Record Retention Policy [under development]
- EA-POL-014 – Enterprise Architecture Policy – Hosting
- EA-POL-015 – Enterprise Architecture Policy – Encryption
- Plymouth University – Information Governance: www.plymouth.ac.uk/your-university/governance/information-governance