ENTERPRISE ARCHITECTURE WITH PLYMOUTH UNIVERSITY

Technology & Information Services

EA-ISP-007 Information Handling Policy

Owner:	Nick Sharratt
Author:	Paul Ferrier
Date:	28/03/2018 07:36:00
Document Security Level:	**PUBLIC**
Document Version:	1.04
Document Ref:	EA-ISP-007
Document Link:	
Review Date:	March 2019

EA-ISP-007 Information Handling Policy

Document Control							
Version	**Author**	**Position**	**Details**	**Date/Time**	**Approved by**	**Position**	**Date/Time**
0.9	Paul Ferrier	Enterprise Security Architect	Initial version drafted	11/02/14	n/a	n/a	n/a
0.91	Steve Furnell / Paul Dowland	Head of School of Computing					
0.92	Paul Ferrier	Enterprise Security Architect	Updated document and reformatted to TIS standard	03/12/2014			
0.93	AH	Head of S&A	Agreed working draft	09/02/2015			
1.00	PW, AH, GB, CD, PF	IT Director	Approved policy	17/02/2015	Paul Westmore	IT Director	17/02/2015 13:50
1.01	PF	ESA	Altered to reflect SM queries	06/03/2015 16:30			
1.02	PF	ESA	Added details around research data destruction	18/03/2015 15:30			
1.03	PW, GB, PF	IT Director, HoS, ESA	Altered wording around research data destruction	01/04/2015 13:40	Paul Westmore	IT Director	01/04/2015 13:40
1.04	PW, GB, NS, PF	IT Director, HoSM, 2x ESA	Prepared document for review	06/03/2018 11:10	Paul Westmore	IT Director	06/03/2018 17:20

EA-ISP-007 Information Handling Policy

Introduction

This policy forms part of the University's Information Security Policy Set and should be read in conjunction with the Information Security Policy (EA-ISP-001) and other supporting documentation.

The Information Handling Policy compliments the Information Security Classification Policy[1] and sets out the requirements on the labelling, storage, transmission, processing and disposal of each type of data. Requirements may include confidentiality (in handling, storage and transmission), integrity (for example, validation processes) and availability (for example, backups). System configuration documentation should itself be classified as **confidential** information.

This policy should be familiar to all staff dealing with information assets.

1. Definitions

Document Owner	The person that is responsible for maintaining the accuracy of the information contained within the document.
Information Asset	Is a body of information, defined and managed as a single unit so it can be understood, shared, protected and exploited efficiently. Information Assets have recognisable and manageable value, risk, content and lifecycles.
Managed service	Is a service that is provided to a known baseline state and subsequently managed entirely by Technology and Information Services.
Provisioned service	Is a service that is provided to a known baseline state and subsequently managed entirely by a non Technology and Information Services service provider.
Public / Standard / Confidential / Restricted information	Please refer to the Information Security Classification Policy[1] for definitions, examples and restrictions surrounding the handling of different types of information.

2. Inventory and Classification of Information Assets

2.1 Technology and Information Services will create and maintain an inventory of all the University's major information assets. The ownership of each asset must be clearly stated.

2.2 When systems are upgraded, reviewed or undergo significant development the maximum classification of its contents will be reassessed, including a privacy impact assessment. All aspects of where the data is stored, processed or transmitted must be included to allow transparent data flow diagrams and system architectures to be documented.

3. Information Protection – Equipment Disposal, Desk, Screen and General

3.1 Damaged storage devices that pertain to a University issued computer, containing confidential or restricted data will undergo an appropriate risk assessment, to determine if the device should be destroyed or repaired. Such devices will remain the property of the organisation and only be removed from site as part of an approved disposal procedure or by the permission of the information asset owner.

3.2 All devices shall be disposed of in line with their data classification.

3.3 When permanently disposing of equipment containing storage media, inclusive of any confidential or restricted data and licensed software the following logic shall be followed:

[1] EIM-POL-001 - Information Classification Policy

If the device **will** be reused	If the device **will not** be reused
Where possible, and dependent of the classification of the data, it will be securely erased from the device. If the device only contains **public** or **standard** information then the standard re-imaging process will render all previous data difficult to recover and shall be sufficient. If this either fails then the storage media will be removed and the media will be rendered unusable either by physical destruction or third party secure deletion.	Depending on the nature and amount of the data will determine whether the storage media will be physically destroyed or a third party will be engaged to perform a secure deletion of the information.

3.4 Any **confidential** or **restricted** data shall always be secured out of sight of unauthorised persons. Paper-based records shall be stored in secure locations and handled in such a way as to prevent unauthorised sight. Screens used to view **confidential** or **restricted** data shall be sited to ensure information cannot be viewed by unauthorised persons.

3.5 Where printing of **restricted** data is permitted, for example Personal Development Records (PDR) or other such documents, secure print functionality must be used (for example, printing to a secure print queue and releasing the job to print with a designated identity card). Unattended printing must not be used for this type of data.

4. Backup, Media and Information Handling

4.1 When a new service is designed, or when a significant upgrade to an existing service is undertaken, the requirements of restoration of service must be considered. This includes the points below:

- 4.1.1 The actual data itself
- 4.1.2 The application which consumes and may transmit or alter the data
- 4.1.3 The server upon which the application is delivered
- 4.1.4 Backups are stored in two locations, onsite for swift restoration and offsite for longer term storage and restoration.

4.2 Technology and Information Services management must ensure safeguards are in place to protect the integrity of information during recovery and restoration of data files; especially where overwriting of more recent versions with older information may occur.

4.3 Technology and Information Services are responsible for backing up all managed and provisioned services. Restoration and/or recovery of any failed services will be conducted in order of business criticality.

4.4 Where services are hosted by third party companies, the backing up and restoration of information must be included as part of the contract for service provision and must be in accordance with both the organisations information security policies and its retention schedule.

4.5 The archiving of information and documents must take place with due consideration for legal, regulatory and business issues, with liaison between technical and business staff, and in keeping with the University's retention policy.

4.6 Storage media used for the archiving of information must be appropriate to its expected longevity. The format in which the data is stored must also be carefully considered and where applicable for **confidential** and **restricted** data encryption must be used.

4.7 All users of information systems must manage the creation, storage, amendment, copying and deletion or destruction of data files in a manner which safeguards and protects the confidentiality, integrity and availability of such files. The degree to which software techniques and disciplined user procedures are necessary shall be defined by the information asset owner (or delegate) and determined by the classification of the information in question.

4.8 Documents that are identified as being **restricted** in readership or be critical to business continuity should not rely upon the availability or integrity of (external) data files over which the author may have no control. Key documents and reports must be self-contained, holding all pertinent information in one place.

4.9 Hard copies of **restricted** materials must be protected and handled according to the distribution and authorisation level specified for those documents.

4.10 All users are to be made aware of the risk of breaching the confidentiality associated with the photocopying, scanning or other duplication of restricted documents. Authorisation from the document owner should be obtained where documents are classified as **confidential** or **restricted**.

4.11 All information used for, or by the organisation, must be filed or stored appropriately and according to its classification.

5. Destruction of Information

5.1 All hard copy documents of a **confident** or **restricted** nature are to be cross-cut shredded or handled in accordance with the Secure Data Destruction Standard[2] when they are no longer required, in line with the University's retention schedule.

5.2 Digital information should be destroyed in a manner that reflects the sensitivity of the data.

5.3 Research data must be securely deleted, in line with the Secure Data Destruction standard[2] and also the HMG InfoSec Standard 5 (enhanced wipe). When the University owned hardware reaches end of life, or fails through the course of its life, it will be physically destroyed.

5.4 Any third party used for external disposal of the University's obsolete information-bearing equipment or hardcopy material must be able to demonstrate compliance with the organisation's information security policies. Additionally, certificates of secure destruction must be provided, and where appropriate, the details of physical destructions carried out when secure destruction fails or is not feasible.

6. Exchanges of Information

6.1 Prior to sending **confidential** or **restricted** information or documents to third parties, not only must the intended recipient be authorised to receive such information, but the procedures and information security measures adopted by the third party, must be seen to assure the continued confidentiality and integrity of the information being exchanged.

6.2 When transferring data or information to either another form of media, or outside of the University's perimeter not only should the Information Security Classification Policy be referenced, but also the Data Transfer Policy[3] where applicable.

6.3 Technology and Information Services Management must ensure that the security of University approved Internet browsers[4], on managed devices, by taking advantage of built-in security features as an absolute minimum and bolstering with additional measures where appropriate.

6.4 All parties are to be notified in advance whenever telephone conversations or videoconference events, such as lectures, are to be recorded.

6.5 Electronic commerce systems, whether to buy or sell goods or services, may only be used in accordance with appropriate technical and procedural measures. Staff authorised to make payment by credit card for goods ordered over the telephone or Internet, are responsible for safe and appropriate use.

6.6 Due care and consideration must be taken when discussing **confidential** or **restricted** material. This exchange should not occur when it can be overheard and subsequently disclosed to other parties, for example, discussing a colleagues' PDR on public transport or in a public area.

---

[2] EA-STD-038 - Secure Data Destruction Standard

[3] EA-POL-012 - Data Transfer Policy

[4] EA-STD-025 - Web Browser Client Desktop Standard

6.7 The identity of recipients or requesters of **confidential** or **restricted** information over the telephone must be verified and they must be authorised to receive it.

7. Information in Application Systems

7.1 Important transactions and processing reports that are exceptions shall be properly escalated for review by properly trained and qualified staff.

8. Specialised Information

8.1 The utilisation of medical data will conform to the Caldicott principles[5].

8.2 Any cardholder data that is stored, processed or transmitted either electronically or physically by members of staff, or parties acting on behalf of the University, will conform to the requirements provided by the Payment Card Industry Data Security Standards (PCI DSS)[6].

[5] Department of Health Caldicott Priniciples: https://www.igt.hscic.gov.uk/Caldicott2Principles.aspx

[6] PCI DSS reference library https://www.pcisecuritystandards.org/document_library?category=pcidss&document=pci_dss