ENTERPRISE ARCHITECTURE WITH PLYMOUTH UNIVERSITY

Technology & Information Services

EA-ISP-007-Information Handling Policy

Owner:	Adrian Hollister
Author:	Paul Ferrier
Date:	01/04/2015
Document Security Level:	**PUBLIC**
Document Version:	1.03
Document Ref:	EA-ISP-007
Document Link:	http://blogs.plymouth.ac.uk/strategyandarchitecture/wp-content/uploads/sites/4/2015/04/EA-ISP-007-Information-Handling-Policy.pdf
Review Date:	December 2015

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

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 Data 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 documentation should itself be classified as **restricted** information.

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

1. Definitions

Document Owner	The person that is responsible for the maintaining the accuracy of the information contained within the document.
Public	These documents should be available for all users, whether internal to the University, a partner or potential partner looking to engage with the University.
Restricted	These documents are either sensitive to a named user, are commercially sensitive or must be only available to specifically named users.
Standard	This classification of document covers all other types of information, they can be distributed within the University; however, if they are to be presented outside to a partner, a non-disclosure agreement must be used.

2. Inventory and Classification of Information Assets

2.1 Technology and Information Services must create and maintain an inventory of all the University's major information assets (for example, any computer that can store, process or transmit standard or restricted information; any piece of University property or equipment that can generate electronic information). The ownership of each asset must be clearly stated.

2.2 When systems are upgraded, reviewed or undergo significant development it is essential that the classification of its contents is reassessed. 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 restricted (or sensitive) 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 When personal storage devices that contain restricted (or sensitive) data, for example a researcher using their own device to conduct work, they must declare this to the University to be recorded as an information asset. Upon completion of the research, confirmation will be required in writing for Technology and Information Services - Service Desk to confirm suitable and secure deletion of the materials have been performed.

3.3 When permanently disposing of equipment containing storage media, inclusive of any 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 the data will be securely erased from the device (as denoted in the **disposal policy when available**). If this either fails, or is likely to take too long to undertake (for example, by imposed timescales from research body), 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 If throughout your role you handle **restricted** (or sensitive, including sensitive personal data) you must adhere to the Clear Desk and Screen Policy (SEC-POL-005). When not required, the data should be stored in a secure location, out of general sight. In addition, screens on which **sensitive** or **restricted** information is processed or viewed should be sited in such a way that they cannot be viewed by unauthorised persons.

3.5 Removal off site of the University's **restricted** (or sensitive) information assets, either printed or held on a digital storage medium (including, but not limited to mobile devices) must be authorised and documented by line management.

3.6 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 mailbox on a printer in open plan offices, or where only the person sending the job can release it for printing). 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 The frequency with which **full** and **differential** backups are required
- 4.1.5 The minimum, acceptable to the business, amount of backups that must be immediately available for restoration. The remainder of the backup information may require additional time to retrieve for use.

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 required services. Through the use of business partners they will ensure that the restoration and recovery, in the event of a failed service, meets the needs of the business.

4.4 Where services are hosted by third parties 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 **restricted** and **sensitive** 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 should be applied by management 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 **standard** or above.

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

4.12 All signatures authorising access to systems or release of information must be properly authenticated.

5. Destruction of Information

5.1 All hard copy documents of a standard or restricted nature are to be cross-cut shred or similarly destroyed 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 (multi pass wipe). When the University owned hardware reaches end of life, or fails through the course of its life, it will be degaussed and then 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, where appropriate, the third party must provide a Service Level Agreement which documents the performance expected and the remedies available in case of non-compliance.

6. Exchanges of Information

6.1 Prior to sending standard 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 Data 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 measure 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

[2] EA-STD-038 - Secure Data Destruction Standard
[3] EA-POL-012 - Data Transfer Policy
[4] EA-STD-025 - Web Browser Client Desktop Standard

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 into account when discussing sensitive or confidential material. This exchange should not occur when it be overheard and subsequently disclosed to other parties, for example, discussing a colleagues' PDR on public transport or in a public area.

6.7 The identity of recipients or requesters of sensitive or confidential 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 must be regularly reviewed by properly trained and qualified staff.

7.2 Email and instant messaging technologies should only be used for business purposes in a way which is consistent with other forms of business communication. When sending attachments that contain user identifying data the attached files need protecting with passwords that are transmitted to the recipient by another form of communication.

8. Specialised Information

8.1 The utilisation of medical data will conform to the Caldicott principles (please refer to the appendix section 7 for further information).

8.2 Any cardholder data that is stored, processed or transmitted either electronically or manually by members of staff will conform to the requirements provided by the Payment Card Industry Data Security Standards (PCI DSS), these are detailed in the Payment Card Security – Information Policy (SEC-POL-003-Payment Card Security)

Appendix

2. Information and Classification of Information Assets

Explanatory Notes
Due to the nature and complexity of certain University systems, it is not anticipated that immediate classification of all data can happen straight away. It is imperative though, that as each system comes under review, or undergoes any substantial developments that the information it stores, processes or transmits is classified in accordance with the University Data Classification Policy.

The overall classification should reflect the highest ranked classified data present (**Restricted**, **Standard** or **Public**)

3. Information Protection – Equipment Disposal, Screen and General

Explanatory Notes
It is important that when data is destroyed it is rendered irretrievable. Use of standard deletion software may be insufficient as it could be possible to use undelete software to restore the data. It is possible that this will increase the actual costs of leasing, loaning or evaluating equipment but this should be factored in to any refresh of equipment.

In some circumstances, information can be recovered from damaged storage devices. In determining how a damaged storage device should be handled, the organisation must assess the risks of the security of the information being compromised. Maintenance contracts for storage equipment should include appropriate undertakings to protect the organisation's information held on devices that are replaced under the terms of such contracts. Specialist organisations can be engaged to undertake and certify the destruction of damaged devices.

Secure disposal of information is the requirement of a number of differing government departments that the University engage in relation to research materials; it is imperative that proof of removal of this data is available when requested by the service providers. Such certification must be stored securely with the Enterprise Security Architect.

With open plan offices now common, an employee may accidentally expose confidential information which could be read from papers on the desk or a visible computer screen. This is a particular risk when staff are away from their desk. A clear desk and screen policy is an effective safeguard.

4. Backup, Media and Information Handling

Explanatory Notes
Adequate backup and recovery procedures ensure information processing can restart successfully after a voluntary or enforced close down.

The need for an appropriate backup regime cannot be over emphasised as it allows the organisation to restore either the whole system or perhaps selected data files, to a specified position. However, the procedures used to initiate such a recovery must be clearly documented and tested – the information security implications of an inappropriate or incorrect restore, are significant.

An organisation may wish to archive documents for various reasons, such as lack of space in a live system, removal of old data that has been processed at the end of a predefined period (end of the month or year), or legal requirements to retain the information. The policy for archiving should be

set by the department that is responsible for determining organisational records policy.
The storage media used for archiving information refers to assets not required on a day to day basis, but which need to be retained for a certain period, and also to information which is retained in perpetuity and referred to infrequently but periodically. Such data is often removed from the day to day live processing.

Secure filing and storage of sensitive material is essential to guard against loss and unauthorised access.

It is critical to establish the signatory's authenticity and level of authority. This policy deals specifically with physical signatures; digital and electronic signatures are covered in the EA-ISP-016 Cryptography Policy.

Unsolicited mail may simply be misaddressed, and therefore returning it to sender may be all that is required. However, staff should be aware that unsolicited physical and electronic mails might be used to probe security systems and to gain unauthorised information.

5. Destruction of Information

Explanatory Notes
All organisations print documents and reports, no longer required hard copy, especially confidential or controlled copies, should be disposed of securely.

When information or data is no longer required by an organisation, it must be deleted or destroyed in a manner that will not contravene legal requirements nor break the terms of any data sharing agreements.

There are specific requirements surrounding the destruction of Patient Identifiable Data, including paper copy being micro cross cut shredding to DIN (Deutsche Industrial Norm) level 5 (maximum cross cut particle size 0.8mm x 12mm) as well as Government Higher Standards for secure data destruction.

6. Exchanges of Information

Explanatory Notes
When sending information to external third parties the principal consideration should be the integrity and confidentiality of the data. In some cases a written agreement setting out responsibilities for the proper handling of the information may be appropriate.

Data may move outside the organisation's control when distributed across networks (both public and private) and by other means, for example the exchange of media such as tapes, disks, optical disks (e.g. CD-ROMs, DVDs etc.) and flash memory (e.g. memory keys). You may wish to consider using encryption techniques to protect the confidentiality of data. If third parties (e.g. couriers) are involved in the transfer these should be selected and managed so as to ensure appropriate levels of information security are maintained.

Web browser software and email software are new paths through an organisation's security shield which could be exploited by an intruder. The security issues are in the areas of cookies, Java applets, JavaScript, ActiveX controls and viruses. The use of a firewall may be unable to protect an organisation from attack via malicious code activated by a web browser.

It is not uncommon for instructions or information to be given over the telephone, but this raises

the issue of verifying the identity of the caller. Be aware of social engineering where the aim is to trick staff into revealing passwords or other information that compromises security.

Electronic commerce provides great opportunities for many organisations, but also involves considerable financial and legal risks. These range from the careless or inappropriate use of company credit cards to financial losses if a price is advertised incorrectly or legal liability if financial details of partners to a transaction are disclosed. Since valid contracts can be created solely by electronic means, any use of electronic commerce must consider who is authorised to enter into such contracts on behalf of the organisation, how they will identify the other party to the transaction and what measures will be used to protect the sensitive data exchanged.

7. Information in Application Systems

Explanatory Notes

The primary systems of the organisation, e.g. the accounting system and other transaction processing systems, should each allow the production of a frequent report, usually daily, that shows the entries processed for the period in question. Such reports should be either printed automatically, or be available on line.

The inherent lack of security for sending information or files appears to be ignored by many, who see the benefits of near instant, and virtually free, global communication as far outweighing any possible downside. Sending email using a digital signature (and optionally being encrypted) is a means of ensuring its validity and integrity to the recipient. The encryption of attachments, through password protection with the password being communicated through another form of media ensures that disclosure of information is minimised.

8. Specialised Data

Explanatory Notes

Caldicott Principles

The Caldicott principles are pertinent to health and social care systems and were published in 1997, they were updated in 2013 and are listed below:

1. **Justify the purpose(s)** – every proposed use or transfer or personal confidential data within or from an organisation should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed, by an appropriate guardian.
2. **Don't use personal confidential data unless it is absolutely necessary** – personal confidential data items should not be included unless it is essential for the specified purpose(s) of that data flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).
3. **Use the minimum necessary personal confidential data** – where use of personal confidential data is considered to be essential, the inclusion of each individual item of data should be considered and justified so that the minimum amount of personal confidential data is transferred or accessible as is necessary for a given function to be carried out.
4. **Access to personal confidential data should be on a strict need-to-know basis** – only those individuals who need access to personal confidential data should have access to it, and they should only have access to the data items that they need to see. This may mean introducing access controls or splitting data flows where one data flow is used for several purposes.
5. **Everyone with access to personal confidential data should be aware of their responsibilities** – action should be taken to ensure that those handling personal confidential data – both clinical and non-clinical staff – are made aware of their responsibilities and obligations to respect patient confidentiality.

6. **Comply with the law** – every use of personal confidential data must be lawful. Someone in each organisation handling personal confidential data should be responsible for ensuring that the organisation complies with legal requirements.
7. **The duty to share information can be as important as the duty to protect patient confidentiality** – health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

These principles will be reviewed on a yearly basis, in order that any amendments can be appropriately amended within this policy document.