ENTERPRISE ARCHITECTURE WITH PLYMOUTH UNIVERSITY

Technology & Information Services

# EA-POL-015 Enterprise Architecture - Encryption Policy


Author: Craig Douglas



Date: 17 March 2015

Document Security Level: **PUBLIC**
Document Version: 1.0
Document Ref: EA-POL-015
Document Link: http://blogs.plymouth.ac.uk/strategyandarchitecture/wp-content/uploads/sites/4/2015/03/EA-POL-015-Enterprise-Architecture-Encryption-Policy.pdf
Review Date: March 2016

# EA-POL-015 Enterprise Architecture - Encryption Policy

## Purpose

The purpose of this policy is to provide Plymouth University with guidance on the use of encryption to protect the Universities information resources that contain, process or transmit information classified as standard or restricted.

## Audience

The intended audience for this policy are all Plymouth University employees, students and other affiliated partners, including contractors.

## Scope

This policy applies to all Plymouth University employees, students and other affiliated partners, including contractors where they are working with, processing, storing or moving University data assets. It addresses encryption policy and controls for standard and restricted data that is at rest (including portable devices and removable media), data in transit (transmission security), and encryption key standards and management.

## Policy

### Encryption Strength

Plymouth University will use FIPS-140-2 validated technologies (e.g. Advanced Encryption Standard (AES), Triple Data Encryption Standard (3DES)[1] (Triple Data Encryption Algorithm (TDEA)), etc.) technologies for encrypting information classified as standard or restricted data under the Plymouth University Data Classification and Management Policy (EIM-POL-001), unless documented through an exception process. Symmetric cryptosystem key lengths must be at least 192 bits or stronger for both standard and restricted data. Asymmetric cryptosystem keys must be of a length that yields equivalent strength (e.g. the US National Institute for Science and Technology (NIST) states that an approximate equivalencies of 256 bit symmetric = 15360 bit asymmetric length[2]). To comply with this policy:

- All encryption mechanisms implemented to comply with this policy support a minimum of but not limited to AES 192-bit encryption.
- The use of proprietary encryption algorithms are not allowed for any purpose, unless reviewed by qualified experts independent of the vendor in question and approved by the Plymouth University Enterprise Security Architect.
- Plymouth University's key length requirements will be reviewed annually and upgraded as technology allows.

### Data at Rest

Hard drives which do not benefit from full disk encryption may have encrypted partitions, the remainder of the disk maybe be logically separated but remain unencrypted, or may connect (or mount) other unencrypted devices. This could lead to information leakage between the secured and unsecured areas and will potentially disclose vulnerable information if interrogated. The hard drives unencrypted auto-recovery folder may retain unencrypted versions or fragments of files that have been saved to the encrypted portion of the disk or USB. The use of full disk encryption avoids this problem, and is currently the only suitable solution approved by Plymouth University.

---

[1] Three 64 bit keys are used, instead of one, for an overall key length of 192 bits (the first encryption is encrypted with second key, and the resulting cipher text is again encrypted with a third key)

[2] NIST Special Publication 800-57 Recommendation for Key Management – Part 1: General (Revision 3). Barker, Barker Burr, Polk and Smid. http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57_part1_rev3_general.pdf

Systems that are likely to hold information, which is classified as standard or restricted and owned or controlled by Plymouth University, must be protected at rest by:

- Full disk encryption
- Firewalls with strict auditable access control that authenticates the identity of individuals accessing the data.
- Complex password protection, as defined in Plymouth University Information Security Policy Supporting Documentation SEC-GDL-003 University Account Passwords[3], should be used in conjunction with encryption and access control. Password control alone is not an acceptable alternative to protecting standard or restricted information.
- Backup solutions, irrespective of media and location must be protected using at least AES 192-bit algorithm based encryption techniques.

All computer hard drives or other storage media that have been encrypted or not shall be sanitised prior to resale or destruction in accordance with the Data Destruction Policy and associated standard.

## Portable Devices

Portable devices represent a specific category of device that contain data-at-rest. A large proportion of information security incidents involving unauthorised exposure of restricted data are as a result of lost or stolen portable computing devices. The best way to prevent these incidents is to avoid storing standard or restricted data on such devices. Restricted data must not be copied or stored on a portable or non-University owned computing device. However, in practice, where a secured remote connection to a University device is not suitable, the use of encryption techniques will reduce the risk of unauthorised disclosure in the event of loss or theft.

When standard or restricted data is to be stored on portable computing equipment (including but not limited to laptops, tablets, smart phones, external hard drives, USB keys etc.):

- Permission must be obtained by the information owner to do so
- The devices in question must be encrypted using methods and products approved by Plymouth University Enterprise Security Architect.
- The devices in question, where appropriate, must have additional security mechanisms in place such as firewall, anti-virus/anti-malware, proper password protection, be fully security patched for all resident software and have unnecessary services and communication ports and protocols switched off.
- Removable media, including but not limited to optical disks, USB memory drives, tape etc. must be encrypted and stored in a secure locked location.
- Transportation of removable media by a 3rd party must be done in a secure manner and a data handling audit trail must be recorded.
- Portable media containing standard or restricted information must be in the possession of an authorised user at all times (e.g. must not be checked in with luggage during transit).

[3] http://blogs.plymouth.ac.uk/strategyandarchitecture/wp-content/uploads/sites/4/2014/06/SEC-GDL-003-University-Account-Passwords.pdf

- The recipient of the removable media must be identified to ensure the person requesting the data is the one claimed.
- Plymouth University will audit encrypted devices and validate implementation of encryption products at regular intervals.
- These devices must not be used for long-term storage of such data, when the data has been processed it is the users responsibility to ensure it has been deleted from the storage media.

## Transmission Security

Users will follow the Plymouth University Enterprise Architecture Policy – Data Transfer (EA-POL-012) when transmitting data and must take particular care when transmitting or re-transmitting restricted information. Information owned by 3rd parties must only be transmitted with the owners' approval and is subject to any additional policies they may have in place.

- Standard or restricted information transmitted by email must be encrypted, with the appropriate password being delivered using a different medium.
- Standard or restricted information transmitted through a public network must be encrypted or transmitted through an encrypted tunnel, such as a SSL or IPSec secured Virtual Private Network (VPN).
- Transmitting unencrypted restricted information through the use of web email software is not permitted.
- Sharing standard or restricted information over Peer-to-Peer (P2P) file-sharing programs requires specific authorisation in writing from both the University Data Protection Officer and Enterprise Security Architect; this will be reported to the Chief Information Officer for sign off before transmission can start.
- Wireless transmission (Wi-Fi) used to access Plymouth University portable computing devices or internal networks must be encrypted using IEEE 802.11i WPA2 (AES) or better.
- Plymouth University permits the secure encrypted transfer of information over the Internet using file transfer programs such as Secured File Transfer Protocol (SFTP over Secure Shell (SSH)) and Secure Copy (SCP). Only authorised devices may perform the SSH/SCP operations, these must be maintained by Technology and Information Systems and are for the use of authorised users only and are subject to the following conditions:
    - Anonymous FTP is not permitted.
    - Standard FTP is not encrypted and must not be used on any Internet facing systems or where standard or restricted data is being transmitted.
    - All accounts and keys must be stored and managed from within the Plymouth University network
    - All transactions and transfers must be logged, and reviewed for prohibited activity
    - All files contained within the managed system or users profile must be deleted within seven days after they are delivered or made available for retrieval.

## Encryption Key Management

Effective key management is essential for ensuring the security and compliance of any encryption system. Key management procedures must ensure that authorised users can access and decrypt all encrypted data using controls that meet operational needs and comply with data retention requirements. Plymouth University key management systems will:

- Use procedures that enforce least privilege concepts and promote separation of duty for support personnel.
- Have verifiable backup solutions for Key passwords, files and other related backup configuration data
- Ensure keys will be transmitted securely only when the requestor is authorised to receive them and has been identified as that individual.
- Adopt key management tools which are fully automated, staff must not have the opportunity to expose the key or influence its creation
- Make provision such that keys in storage and transit must themselves be encrypted.
- Private keys must be kept confidential
- Keys must be randomly generated using hardware based randomisation
- Key used for the encrypting of other keys must be maintained separately from data keys
- A complete audit trail of all key management activities must be maintained and stored securely as defined in the Records Retention Data Storage Schedule.

## Exception Management

Exceptions to this policy may be granted using the Enterprise Architecture Waiver Process and will be considered by the Enterprise Security Architect on merit, risk to University classified standard or restricted information, as well as alignment with the overall security architecture.

Failure to comply with this policy may lead to the solution architecture being rejected during Enterprise Architecture review, returned for rework or placed on hold. In circumstances where failure to comply leads to a breach of information security or of significant risk of the same, disciplinary action may be taken due to the terms of employment being breached. In addition, any systems configured in a manner that contravenes this policy and other related policies will be disabled pending investigation.

## Supporting Documentation

This policy is supported by established Enterprise Architecture documents, namely:

- Enterprise Architecture Principles - Principle 8: Data Security
    - “Security must be designed into data elements from the beginning; it cannot be added later. Systems, data, and technologies must be protected from unauthorised access and manipulation. Vice Chancellor’s Executive information must be safeguarded against inadvertent or unauthorised alteration, sabotage, disaster, or disclosure.”
- Enterprise Architecture Principles - Principle 9: Data is an Asset
    - “Accurate, timely data is critical to accurate, timely decisions. Most corporate assets are carefully managed, and data is no exception. Data is the foundation of our decision-making, so we must also carefully manage data to ensure that we know where it is, can rely upon its accuracy, and can obtain it when and where we need it, in doing so data assets can provide additional value to academic and research endeavors.”

- Enterprise Architecture Principles - Principle 10: Data is Shared
    - "Data where applicable, will be available externally to the enterprise. This will afford both rich service provision also the ability to perform research collaboratively with partners."
- Enterprise Architecture Principle – Principle 11: Data is Accessible
    - "Wide access to data leads to efficiency and effectiveness in decision-making, and affords timely response to information requests and service delivery. Using information must be considered from an enterprise perspective to allow access by a wide variety of users. Staff time is saved and consistency of data is improved."
- Enterprise Architecture Principles – Principle 17: Data will be Analysable
    - Data assets provide invaluable information to the enterprise for research and business intelligence decision-making when gathered, stored and accessed correctly."
- EA-POL-012 – Enterprise Architecture Policy – Data Transfer
    - "Secure protocols will always be used in preference over unsecured protocols for data transmission. If no secured protocol is available then a secured tunneling (IPSec or SSL VPN) technique must be utilised to prevent information being transmitted in plain sight of network users."
- SEC-GDL-003 – University Account Passwords
    - University password requirements
- EIM-POL-001 - Data Classification and Management Policy
    - 3. Assigning classification levels

| Document Control | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Version** | **Author** | **Position** | **Details** | **Date/Time** | **Approved by** | **Position** | **Date/Time** |
| 0.1 | Craig Douglas | Enterprise Architect | Initial Document | 18 September 2014 | | | |
| 0.2 | Craig Douglas | Enterprise Architect | Update following EAP Review | 13 October 2014 | | | |
| 0.3 | Craig Douglas | Enterprise Architect | Updated Template | 14 January 2015 | | | |
| 0.4 | Paul Ferrier | Enterprise Security Architect | Updated a number of links | 12 February 2015 | | | |
| 1.0 | PW, AH, GB, CD, PF | IT Director, HoS, EA | Approved policy | 13 March 2015 | Paul Westmore | IT Director | 13/03/2015 12:25 |