ENTERPRISE ARCHITECTURE WITH PLYMOUTH UNIVERSITY

Technology & Information Services

EA-POL-015 – Encryption Policy (Abridged Version)

Author: Paul Ferrier

Date: 28/10/2016

Document Security Level: **PUBLIC**
Document Version: 1.0
Document Ref: EA-POL-015 - Encryption Policy Abridged Version
Document Link:
Review Date: October 2017

EA-POL-015 – Encryption Policy (Abridged Version)

Device encryption

If you are storing, processing or transmitting either **confidential** or **restricted** information on your computer (irrespective of whether it is a laptop, desktop, tablet or mobile phone) the device should be encrypted.

Portable devices (including USB sticks, for example) are very easy to use for transporting information from one location to another, however it is more likely that these devices could be lost or mislaid. Therefore, appropriate measure should be taken, this could be encrypting certain files with passwords or the entire disk.

Sending information digitally

Emails are not secure, if there is a requirement to send **confidential** or **restricted** data through this mean, the attached files must be encrypted[1] (password protected) and the key provided to the recipient via another means (telephone call for example).

When providing a username and password to access University systems, or completing forms that require personal or sensitive personal information, secured websites or applications must be used.

Encryption strength

Encryption protocols and cryptographic algorithms that protect University data in transit will be maintained on University managed computers in line with current industry best practice.

References

Further, more detailed technical information is available in the following documents:

EA-POL-015 - Enterprise Architecture Encryption Policy

EIM-POL-001 - Information Security Classification Policy

[1] http://blogs.plymouth.ac.uk/strategyandarchitecture/wp-content/uploads/sites/4/2014/06/SEC-GDL-007-Document-Encryption.pdf