ENTERPRISE ARCHITECTURE WITH PLYMOUTH UNIVERSITY

Technology & Information Services

EA-ISP-016-Cryptography Policy

Owner:	Adrian Hollister
Author:	Paul Ferrier
Date:	17/03/2015
Document Security Level:	**PUBLIC**
Document Version:	1.0
Document Ref:	EA-ISP-016
Document Link:	http://blogs.plymouth.ac.uk/strategyandarchitecture/wp-content/uploads/sites/4/2015/03/EA-ISP-016-Cryptography-Policy.pdf
Review Date:	March 2016

Document Control							
Version	**Author**	**Position**	**Details**	**Date/Time**	**Approved by**	**Position**	**Date/Time**
0.9	Paul Ferrier	Enterprise Security Architect	Initial version created	27/03/2014			
0.91	Paul Ferrier	Enterprise Security Architect	Transposed into new document format	12/02/2015			
1.00	PW, AH, GB, CD, PF	IT Director, HoS, EA	Approved policy	13/03/2015	Paul Westmore	IT Director	13/03/2015 12:20

EA-ISP-016-Cryptography 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, including the Enterprise Architecture Policy surrounding Encryption (EA-POL-015[1]).

The Cryptography Policy sets out when and how encryption should (or should not) be used. It includes protection of restricted (or sensitive) information and communications, key management, and procedures to ensure encrypted information can be recovered by the organisation if necessary.

Please refer to the appendix for further explanation of the points below.

1. Cryptography and compliance

1.1 Policies, standards and procedures will be developed to provide appropriate levels of protection for organisational data whilst ensuring compliance with statutory, regulatory and contractual requirements.

2. Use of encryption

2.1 Restricted information shall only be taken for use away from the organisation in an encrypted form unless its confidentiality can otherwise be assured.

2.2 Procedures shall be established to ensure that authorised staff may gain access, when needed, to any important business information being held in an encrypted form.

2.3 The confidentiality of information being transferred on portable media or across networks must be protected by use of appropriate encryption techniques.

3. Managing electronic keys

3.1 A procedure for the management of electronic keys, to control both the encryption and decryption of restricted (or sensitive) documents or digital signatures, must be established to ensure the adoption of best practice guidelines and compliance with both legal and contractual requirements

4. Using and receiving digital signatures

4.1 Important business information being communicated electronically shall be authenticated by the use of digital signatures; information received without a digital signature should be dealt with carefully until verified by the sending individual, if it seems out of character with previously received communications.

[1] Enterprise Architecture Encryption Policy

Appendix

1. Cryptography and compliance

Explanatory Notes

Whilst the initial reason for embarking on a cryptography policy might be the protection of restricted (confidential or sensitive) information, cryptography also offers benefits in such areas as e-Commerce.

2. Use of encryption

Explanatory Notes

Confidential information on a mobile device (laptop, iPad or smartphone for example) taken from the office, for a meeting or to work at home, is exposed to greater security threats – the device may be stolen or a family member might use it.

Also, data on devices used in external events, such as student enrolments at partner organisations, might also be at risk, information security risks should be assessed and encryption employed where it is found appropriate.

In the normal course of business it might be desirable for a member of staff to hold some important confidential data securely in an encrypted form. It is essential, however, that this data remains accessible in their absence. Staff might be required a use a shared group pass-phrase to protect such data, a record of pass-phrases could be held in a secure repository, or staff may be required to encrypt using an organisational public key as well as their own.

Confidential data distributed across networks (both public and private) and by other means, e.g. tapes, disks, CDs, DVDs and USB keys, needs appropriate protection to assure confidentiality and integrity.

Remote users, either teleworkers or personnel on business trips etc., may need to communicate directly with their organisations' systems to receive/send data and updates. Such users are physically remote and often connect through public (insecure) networks. This increases the threat of unauthorised access. Remote access was traditionally provided by means of dial-up or leased phone lines. Today, however, VPNs provide access across public networks, e.g. the internet.

3. Managing electronic keys

Explanatory Notes

Electronic keys are used to encrypt and decrypt messages or digital signatures on messages sent between one or more parties. The management of the electronic keys is critical if confidentiality, authenticity and integrity are to be preserved.

4. Using and receiving digital signatures

Explanatory Notes

The option of using digital signatures in electronic documents can provide a means of introducing a high degree of authenticity and integrity to an otherwise insecure communications medium. Confidence can be had in an email sent using an appropriate digital signature – its contents only need encrypting if it is also restricted (or confidential). The content of emails received without signatures may be considered unreliable.

When using digital signatures, consideration must be given to any relevant legislation that describes the conditions under which a digital signature is legally binding.