ENTERPRISE ARCHITECTURE WITH PLYMOUTH UNIVERSITY

Technology & Information Services

EA-ISP-016 Cryptography Policy

Owner:	Nick Sharratt
Author:	Paul Ferrier
Date:	08/03/2018
Document Security Level:	**PUBLIC**
Document Version:	1.10
Document Ref:	EA-ISP-016
Document Link:	
Review Date:	March 2019

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
1.10	PW, GB, NS, PF	IT Director, HoSM, 2 x ESA	Updated ahead of review	06/03/2018	Paul Westmore	IT Director	06/03/2018 17:20

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 the protection of **confidential** and **restricted** information and communications, key management, and procedures to ensure encrypted information can be recovered by the organisation if necessary.

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.

2.4 The University is moving towards a paradigm of encryption by default, all new services should be able to adopt this concept to protect the confidentiality and integrity of the information that it ingests, stores and/or distributes.

2.5 The offsite backup of University systems and data will be encrypted before being transmitted out of the organisation. The encryption keys will be retained to ensure the hosting provider has no access to the University's data.

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.

[1] Enterprise Architecture Encryption Policy