ENTERPRISE ARCHITECTURE WITH PLYMOUTH UNIVERSITY

Technology & Information Services

EA-ISP-004 Outsourcing and Third Party Access

Owner:	Nick Sharratt
Author:	Paul Ferrier
Date:	28/03/2018 07:35:00
Document Security Level:	**PUBLIC**
Document Version:	1.10
Document Ref:	EA-ISP-004
Document Link:	
Review Date:	March 2019

EA-ISP-004 Outsourcing and Third Party Access

Document Control							
Version	**Author**	**Position**	**Details**	**Date/Time**	**Approved by**	**Position**	**Date/Time**
0.90	Paul Ferrier	Enterprise Security Architect	Created the document	19/03/2014			
0.91	Steve Furnell and Paul Dowland	Head of School of Computing, Associate Professor	Peer review and comments	10/04/2014			
0.92	Nicola Tricker, Emma Brewer and Adrian Jane	Supplier Manager, Supplier Liaison Administrator and Third Party Service Provision Manager	Peer review and comments	25/11/2014			
0.93	Paul Ferrier	Enterprise Security Architect	Alteration following Hosting Policy changes	16/01/2015 14:20			
1.00	PW, AH, GB, CD, PF	Interim IT Director	Approved sign off	17/02/2015 16:55	Paul Westmore	Interim IT Director	17/02/2015 13:30
1.01	PF	ESA	Correction of links	06/03/2015 15:10			
1.02	PF	ESA	Updated for 2018	07/06/2017 14:35			
1.10	PW, GB, NS, PF	IT Director, HoSM, 2x ESA	Tweaked for formal review	06/03/2018 14:45	Paul Westmore	IT Director	06/03/2018 17:20

EA-ISP-004 Outsourcing and Third Party Access

Introduction

This information security policy document sets out principles and expectations about maintaining the security of Plymouth University IT facilities that are accessed, managed, supported or provided by third parties. It is a sub-document of the Information Security Policy (EA-ISP-001) and should be read in conjunction with the Information Security Classification Policy (EIM-POL-001).

1. Definitions

Confidential information	is information that if improperly disclosed or lost could cause harm to the business or an individual. This includes personal data as identified by the Data Protection Act and other value or sensitive information that is not in the public domain.
Third parties	are external organisations or individuals other than the University's own staff or students.

2. Contractual Issues

2.1 All third parties who are given access to the University's information systems, whether as suppliers, customers or otherwise, must agree to follow the information security policies of the organisation. An appropriate summary of the information security policies and the third party's role in ensuring compliance must be formally delivered to any such third party, prior to being granted access.

2.2 Non-Disclosure Agreements (NDAs) shall be used in all situations where the confidentiality, sensitivity or value of the information being disclosed is classified as **Confidential** or **Restricted**[1].

2.3 All contracts with third parties to supply, manage or facilitate service are subject to University of Plymouth performing audits (either directly, or via a specialist third party auditor) to ensure compliance with information security requirements. This may be in the form of planned or no-notice inspections.

2.4 All contracts must include appropriate provisions to ensure the continued security of information and systems in the event that a contract is terminated or transferred to another supplier.

2.5 All contracting third parties must disclose any fourth (or subsequent) parties that they themselves subcontract to in order to form an understanding of supply chains.

3. Third Party Development, Maintenance and Support

3.1 Persons responsible for commissioning outsourced development of computer-based systems and services must use reputable companies that operate in accordance with quality standards, as denoted by ISO27001 accreditation or equivalent. These companies will be required to follow the information security policies of this organisation, in particular those relating to application development.

3.2 Persons responsible for agreeing maintenance and support contracts will ensure that the contracts being signed are in accord with the contents and spirit of the University's information security policies.

3.3 Any maintenance undertaken by a third party, must be agreed and timetabled with all concerned parties prior to the engagement in any work itself.

3.4 All third parties must use discretion when creating or managing credentials to administer the service. Default user names can only be used when no alternative is available and passwords must be randomly generated and contain uppercase, lowercase, numeric and special characters with a minimum length of fifteen characters. If the system or service is unable to support this, consultation

[1] As derived from the Information Security Classification Policy

must be sought to agree a minimum standard of complexity suitable for the system. No default system passwords must ever be used in any state of development, test or live service.

3.5 If access is required to University of Plymouth assets within its perimeter, communications must be secured through approved mechanisms for remote access[2] and/or data transfer[3].

3.6 All third parties who provide payment related services (including cardholder data processing, transmission and storage) must be compliant with the current Payment Card Industry Data Security Standards (PCI DSS). This data will not be held within the University environment and must be managed entirely by the third party.

3.7 Any Information Security breaches that occur against a third party provider of service must be conveyed to the University, through the Enterprise Security team or Data Protection Specialist within the agreed priority one incident level (as denoted in the Service Level Agreement) or at the earliest available opportunity, whichever is sooner. When the breach has been remedied, a report detailing the steps taken and any measures that will prevent the breach from occurring again should also be provided to the University, within a maximum period of ten working days.

4. Third Party Service Provision

4.1 Any outsourcing or similar company with which this organisation may do business must be able to demonstrate compliance with the organisation's information security policies and enter in to binding service level agreements that specify the required performance and appropriate remedies available in the case of non-compliance.

[2] Remote Access Policy
[3] Data Transfer Policy