ENTERPRISE ARCHITECTURE WITH PLYMOUTH UNIVERSITY

Technology & Information Services

EA-ISP-005 Personnel IT Policy

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-005
Document Link:	
Review Date:	March 2019

Document Control							
Version	**Author**	**Position**	**Details**	**Date/Time**	**Approved by**	**Position**	**Date/Time**
0.90	PF	Enterprise Security Architect	Initial draft	08/02/2014			
0.91	LT, KE, PF	Head of HR Operations, HR Operations and System Specialist	Updates following review with TOD	28/02/2014			
0.92	PF	Enterprise Security Architect	Completed appendix for explanatory notes	19/03/2014			
0.93	PF	Enterprise Security Architect	Transferred to new template and added role information for Confidentiality agreements	10/02/2015			
1.00	PW, AH, GB, CD, PF	Interim IT Director	Approved document	17/02/2015 17:05	Paul Westmore	Interim IT Director	17/02/2015 13:35
1.01	PF	ESA	Updated the policy ahead of formal review	05/12/2017 13:40			
1.10	PW, GB, NS, PF	IT Director, HoSM, 2 x ESA	Formal review of policy	06/03/2018	Paul Westmore	IT Director	06/03/2018 17:20

EA-ISP-005 Personnel IT Policy

Introduction

The Personnel Policy sets out the processes and responsibilities that are necessary to ensure that the staff of the university contribute to the security of its information.

Depending on their role within the university, different individuals will have different levels of responsibility for information security, but in all cases these responsibilities need to be defined and individuals given appropriate training and support to enable them to fulfil their responsibilities.

1. Security related to position

1.1 The Terms and Conditions of Employment of the University include the employer's and employee's requirements to comply with information security policies.

1.2 All employees are required to sign a formal undertaking concerning the need to protect the confidentiality of information, both during and after their employment with the University.

2. Recruitment, references and screening

2.1 All those contracted for services to the University must agree to follow the information security policies of the University. An appropriate summary of the information security policies must be formerly delivered to any such supplier prior to the provision of services.

3. Confidentiality agreement

3.1 Non-disclosure agreements must be used in all situations where the confidentiality, sensitivity or value of the information being disclosed is important to the University.

3.2 Confidentiality agreements are drawn up, catalogued and signed off through the University's specialist advisor on Intellectual Property who works within the Research and Innovation directorate.

4. Information security education and training

4.1 All existing staff are to be provided with information security awareness training on an annual basis. The aim of this is to enhance and maintain awareness, educating users to the range of active threats to our environment, any appropriate safeguards to protect data and the need to report suspected problems.

4.2 As part of the induction process, for full, part time or temporary staff, an appropriate summary of the information security policies must be formerly delivered and accepted by any individual, prior to the supply of services.

4.3 When a member of staff changes their job, the information security needs of the individual in their new role must be addressed, any new training provided as a priority and any old permissions no longer required must be removed.

4.4 The University is committed to providing training to all users of new systems to ensure that their use is both efficient and does not compromise information security.

4.5 Specific awareness training surrounding data protection or information security will be provided, if required, as part of any engagement with research projects and its associated data.

5. Disgruntled or departing staff

5.1 Management must respond quickly, yet discreetly to indications of disgruntled staff, liaising as necessary with Human Resources management and the Enterprise Security team.

5.2 Upon notification of staff resignations, contract termination or retirement, Human Resources must consider, with the Enterprise Security team if required, whether the member of staffs continued system access rights constitutes an unacceptable risk to the organisation and, if so, revoke all access rights.

5.3 Departing staff must return all information assets and equipment belonging to the University for the destruction of data on electronic devices, unless agreed otherwise with the designated owner responsible for the information asset.

5.4 Departing staff will have their access privileges terminated promptly through Service Management's procedure for account disabling and this should be undertaken with a modicum of discretion.

6. Disciplinary Process

6.1 If, after investigation, a user is found to have violated the University's information security policies and/or procedures they may be disciplined in line with the University's formal disciplinary process.