ENTERPRISE
ARCHITECTURE
WITH
PLYMOUTH
UNIVERSITY

Technology & Information Services

# EA-ISP-005-Personnel IT Policy

| | |
|---|---|
| Owner: | Adrian Hollister |
| Author: | Paul Ferrier |
| Date: | 17/02/2015 |
| | |
| Document Security Level: | **PUBLIC** |
| Document Version: | 1.00 |
| Document Ref: | EA-ISP-005 |
| Document Link: | http://blogs.plymouth.ac.uk/strategyandarchitecture/wp-content/uploads/sites/4/2015/02/EA-ISP-005-Personnel-IT-Policy.pdf |
| Review Date: | February 2016 |

| 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 |

# 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.

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

## 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 awareness and educate the users regarding the range of threats, the appropriate safeguards and the need for reporting 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 must be readdressed and any new training provided as a priority.

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 Talent and Organisational Development management and the Enterprise Security Architect.

5.2 Upon notification of staff resignations, contract termination or retirement, Talent and Organisational Development must consider, with the Enterprise Security Architect 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.

# Appendix

## 1. Security in job descriptions

### Explanatory Notes

All employees are required to comply with all information security policies.

The Terms and Conditions of Employment specify the particulars of the employment relationship between an employer and employee. All such documentation usually covers certain basic issues, but their content may also vary because what is deemed necessary for inclusion depends on the type of organisation, the position, and so forth. Standard contracts of employment are redrafted from time to time to ensure that they keep up with changing times increasingly the issue of information security is being recognised as one that should be expressly addressed in modern contracts of employment.

A key aspect of any information security process is the maintenance of confidentiality of information and data.

## 2. Recruitment, references and screening

### Explanatory Notes

Employers must protect themselves against hiring individuals who are ill suited to the demands of the job. All employers are likely to be given access to the organisation's Information Systems, and therefore the resultant information security risks need to be addressed. Care must be taken in assigning security clearance levels to staff members and also in checking the validity of their references.

Adequate security constraints may be in force for employees and contractors, but those same levels of safeguard maybe overlooked when dealing with third parties, such as hardware and software suppliers, consultants and other service providers.

## 3. Confidentiality agreements

### Explanatory Notes

It is common practice to use a non-disclosure agreement or NDA as a legally enforceable means of redress to prevent a third party inappropriately communicating confidential information covered by the NDA to an unauthorised party. All staff and contractors should sign contracts of employment with non-disclosure clauses duly inserted.

## 4. Information security education and training

### Explanatory Notes

It only takes a single lapse to put your organisation's data and information resources at risk. Organisations should therefore aim to develop their staff's awareness of information security risks so that good practice becomes second nature. Staff should also be aware of the importance of promptly reporting, through appropriate management channels, any security incident or suspected weakness and procedures should be in place to respond to, and learn from, reported weaknesses.

Third party contractors coming into the organisation are usually specialists or professionals, and it is easy to assume that their expertise also extends to information security. In fact, the converse is true; they are less likely to appreciate your organisational information security arrangements.

Permanent staff should be aware of the risks posed by such third party contractors on their site.

Temporary staff members are viewed as a transient resource that is used to maximise productivity and minimise costs. Although they have access to company information, they are not usually held accountable for their actions, as they are not part of the company. This increases the risk of information security breaches.

The introduction of new information systems presents risks for information security. New user interfaces may be misunderstood, resulting information being deleted or processed incorrectly. New systems may require different security measures to be taken by staff using them. Staff who are not adequately trained in these aspects of new systems may accidentally damage security.

All management and staff are responsible for information security, including those new to the organisation. It is vital that new staff are brought up to speed quickly to avoid information security breaches. The level of training required must be appropriate to their specific duties, so that confidentiality, integrity and availability of information they would normally handle is safeguarded.

By virtue of their position, technical staff both protect the organisation’s information, but equally, may inadvertently (or maliciously) put it at greater risk. Therefore it is essential that they be trained to a level of competence in information security that matches their duties and responsibilities.

## 5. Departing staff

### Explanatory Notes

Disgruntled staff can present a significant risk as they are still deemed trusted employees, but their potential to inflict damage is high. All staff will normally be aware of what information assets are of value to the organisation and, although they may not have direct access themselves, they may be able to obtain access through personal relationships.

Staff resignations occur from time to time and in the main are harmonious. However, whenever a member of staff resigns, there is the possibility that the person may be resentful of some issue, and could subsequently potentially act in a manner which could jeopardise the security of the organisation.

Information assets may consist of paper or electronic files, or be stored in equipment such as laptops, mobile phones or other storage devices. It is safest to require that all of these be returned – the organisation can then control whether, and under what conditions, it allows the departing member of staff to retain a copy. This is particularly important where a member of staff has been involved in mobile working or teleworking, or has used their own equipment to store or process the organisation’s information in some cases, particularly where confidential information has been processed, it may be necessary to have the departing person sign a declaration that no copies of information have been retained.

Staff who resign should be treated sensitively or they may become disgruntled and/or simply leave without adequate hand over to colleagues, etc.

## 6. Disciplinary process

### Explanatory Notes

Violation of the organisation’s information security policy and procedures should be dealt with under the organisation’s formal disciplinary process.