ENTERPRISE ARCHITECTURE WITH PLYMOUTH UNIVERSITY

Technology & Information Services

EA-ISP-003-Compliance Policy

Owner:	Adrian Hollister
Author:	Paul Ferrier
Date:	17/02/2015
Document Security Level:	**PUBLIC**
Document Version:	1.01
Document Ref:	EA-ISP-003
Document Link:	http://blogs.plymouth.ac.uk/strategyandarchitecture/wp-content/uploads/sites/4/2015/01/EA-ISP-003-Compliance-Policy.pdf
Review Date:	February 2016

Document Control							
Version	**Author**	**Position**	**Details**	**Date/Time**	**Approved by**	**Position**	**Date/Time**
0.90	Paul Ferrier	Enterprise Security Architect	Created the document	10/02/2014			
0.91	Steve Furnell and Paul Dowland	Head of School of Computing / Senior Professor	Academic Review	February 2014			
0.92	PF, SW, CD, KW	Technical Architecture Group	Conversation around policy and amendments	07/03/2014			
0.93	PF	Enterprise Security Architect	Inclusion of appendix for reference notes				
0.94	AH	Head of S&A	Agreed working draft	09/02/2015			
1.00	PW, AH, GB, CD, PF	Interim IT Director, Head of Strategy & Architecture	Approved document	17/02/2015 16:25	Paul Westmore	Interim IT Director	17/02/2015 13:25
1.01	PF	ESA	Inclusion of IP Policy and Data Retention information	06/03/2015 09:55			

EA-ISP-003-Compliance 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, such as the Data Classification Policy.

The Compliance Policy aims to ensure both compliance with legal obligations and compliance with the organisations own information security standards. The policy document sets out the processes for identifying any legal obligations which may bind the organisation; defines measures to avoid any breaches of those obligations; and describes the controls necessary to ensure that the standards in the organisation security policy are met.

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

1. Awareness of Legal Obligations

1.1 For each University department, a nominated co-ordinator is responsible for communicating guidelines and any changes to ensure that all staff comply with their legal responsibilities in respect of their use of computer based information systems and data; this should be disseminated to their student cohort where appropriate in teaching activities. Such responsibilities are to be included within key staff and student documentation such as Terms and Conditions of Employment and the Organisation Code of Conduct.

1.2 System planning processes explicitly define and document the legal obligations arising from the operation of the proposed system. There is a named individual, per department responsible for updating that information.

2. Ensuring Compliance with Legal Obligations

2.1 The organisation will comply fully with the requirements of data protection legislation.

2.2 It is the responsibility of all authors who make or publish materials to be aware of the Intellectual Property and Copyright restrictions outlined by the Research and Innovation directorate[1].

2.3 The information created or stored within the organisation's information systems must be retained for a minimum period that meets both legal and business requirements. The organisation should maintain a suitable archiving and record retention procedure.

2.4 Data retention periods[2] for data and information must be established to meet legal and business requirements and must be adhered to by all staff.

2.5 The archiving of documents must take place with due consideration for legal, regulatory or business issues and must be transparent to the users responsible for the archiving process.

2.6 Information regarding the organisation's applicants, students, suppliers and other people dealing with the organisation is to be kept restricted (confidential) and must be protected and safeguarded from unauthorised access and disclosure.

2.7 The organisation via Talent and Organisational Development are to ensure that all employees are fully aware of their legal and corporate duties and responsibilities concerning the inappropriate sharing and releasing of information, both internally within the organisation and external parties.

2.8 The Enterprise Security Architect (ESA) or nominee is responsible for preparing guidelines to ensure that all staff and students are aware of the key aspects of computer misuse legislation (or its equivalent), in so far as these requirements impact on their duties.

3. Evidence

3.1 Where it is necessary to gather evidence to support an investigation, surrounding a person or

[1] Research and Innovation - IP Policy
[2] EIM-POL-004 Record Retention Schedule

organisation, it shall be collected and presented to conform to the relevant rules of evidence. Expert guidance will normally be sought.

4. Ensuring Compliance with Organisational Security Policy

4.1 All staff and students are required to comply fully with the organisation's information security policies. The monitoring of such compliance is the responsibility of management at all levels.

4.2 The organisation's systems must be operated and administered using documented procedures in a manner which is both efficient but also effective in protecting the organisation's information security.

4.3 All systems must be regularly checked, through the Enterprise Architecture Compliance review to ensure that they comply with the organisational security policy.

4.4 The organisation will appropriately apportion a number of services or systems, held locally or by third parties to be audited within a calendar year for compliance with information security policy. System owners will be notified with a minimum of six weeks before the internal audit commences.

Appendix

1. Awareness of Legal Obligations

Explanatory Notes

Awareness of legal aspects of using computer based information systems is important so that users do not inadvertently contravene legal requirements. Familiarity with legal requirements relevant to your duties and functions should be a requirement of your organisation's Information Security Policy.

Before new systems are introduced, it is important for the organisation to fully understand the legal obligations that will arise from the operation of the system. These may be regulatory, contractual or common law obligations and they may change over time.

A named person or role should be responsible for keeping these legal obligations under review. They must update the relevant documentation and notify any staff who are affected should there be any change.

2. Ensuring Compliance with Legal Obligations

Explanatory Notes

The protection of copyright is a global issue. The simple act of copying copyrighted material constitutes a breach of the law. Infringement of copyright in the course of business is a criminal matter; even without selling such copies. By merely using them, you could risk imprisonment and damages or compensation.

In many countries there is also legislation covering the protection of information held in databases. These database rights cover owner and user rights, both for online and paper based databases.

A contractual agreement setting out what can and cannot be done to a database is a way of minimising the risk of legal action by users or owners of databases.

Copying and distributing software is illegal, unless permission is expressly granted by the owner of the copyright in that software.

Retention of particular types of records and storage of media may be a legal requirement and, with regards to personal data, deletion of the records may be required after their usefulness has come to an end. It may also be necessary to keep other types of records and to ensure that they remain accessible for a period of time for business efficacy.

You may wish to archive documents for various reasons, such as: lack of space in the live system, removal of old data that has been processed at the end of a predefined period (end of the month or year), or legal requirements to retain the information. The policy for archiving should be set for the department that is responsible for determining the organisations records policy.

Whereas the filing of printed business correspondence is often performed centrally, the management of email boxes is often performed individually or by a group. However, it may not be clear what email correspondence should be retained.

Data protection legislation normally covers all types of information which may be in either electronic form or held as manual records. The legislation normally relates to the protection of the rights of individual persons. In many countries it also covers medical records although increasingly this type of

information is governed by separate legislation. Internationally, data protection has become an important issue. This policy covers its relevance to staff and third parties.

Keeping this type of information confidential is both a legal requirement and essential for organisational credibility.

Sharing information between different divisions, groups or sections of your organisation is often necessary for the business or organisation to function. This raises information security issues.

Casual comments in emails relating to individuals or rival companies may be construed as defamatory – even if the comments are valid.

The legal consequences for publishing potentially defamatory material on an open access medium, such as the internet, can be severe.

3. Evidence

Explanatory Notes

Where an organisation is to successfully pursue an action or to defend itself when an action is brought against it, evidence is normally required. Increasingly this information will be contained within information systems and special consideration must be given to how the authenticity and accuracy of the information can be established. Expert guidance should normally be sought.

4. Ensuring Compliance with Organisational Security Policy

Explanatory Notes

Compliance with your organisation's information security policy is mandatory for all users.

The means by which your IT systems are run and maintained on a day to day basis must comply with legal and contractual requirements.

IT facilities should be regularly checked for compliance with security implementation standards.