FALMOUTH UNIVERSITY

Falmouth Exeter Plus

Information Security Policy

Information Security Policy
2016

Falmouth Exeter Plus
Falmouth University
Information Security
Policy

Title :	**Information Security Policy**
Document Reference :	**ISP001**
Status :	**Draft**
Version :	**0.2**
Date :	**June 2016**
Classification :	**Public**

Contents

Introduction 2

Purpose 2

Scope 2

Structure 2

Information Security Principles 3

Governance 3

Sub-Policies 3

Introduction

Information is a vital asset to any organisation and this is especially so in a service delivery organisation such as the Falmouth Exeter Plus (FX Plus) and a higher education establishment such as Falmouth University, where information will relate to learning and teaching, research, administration and management. This policy is concerned with the management and security of the organisation's information assets (an information asset is defined to be an item or body of information, an information storage system or an information processing system which is of value to either organisation) and the use made of these assets by their staff/students and others who may legitimately process information on behalf of the organisation.

This overarching policy document provides an overview of information security and lists a hierarchical set of policy documents (sub-policies) which taken together constitute the Information Security Policy of both Falmouth University and Falmouth Exeter Plus.

Purpose

An effective Information Security Policy provides a sound basis for defining and regulating the management of information systems and other information assets. This is necessary to ensure that information is appropriately secured against the adverse effects of failures in confidentiality, integrity, availability and compliance which would otherwise occur.

Scope

The documents in the Information Security Policy set apply to all information assets which are owned by Falmouth University and FX Plus, used by organisations, or their partners, for business purposes or which are connected to any networks managed by FX Plus.

The documents in the Information Security Policy set apply to all information which the organisations process, irrespective of ownership or form.

The documents in the Information Security Policy set apply to all members of staff within of FX Plus, and all staff and students of Falmouth University

Structure

The Information Security Policy document set is structured in accordance with the recommendations set out in the "UCISA Information Security Toolkit" which in turn, is based on the control guidelines set out in the industry standard ISO 27001.

This top level document lists a set of other sub-policy documents which together constitute the Information Security Policy of FX Plus and Falmouth University. All of these documents are of equal standing. Although this policy set should be internally consistent, for the removal of any doubt, if any inconsistency is found between this overarching policy and any of the sub-policies, this overarching policy will take precedence.

Each of the sub-policy documents only contains high-level descriptions of requirements and principles. They do not, and are not intended to include detailed descriptions of

policy implementation. Such details will, where necessary, be supplied in the form of separate procedural documents which will be referenced from the relevant, individual sub-policy documents

Information Security Principles

Falmouth Exeter Plus and Falmouth University will adopt the following principles to underpin this policy:

- Information will be protected in line with all relevant organisational policies and legislation, notably those relating to data protection, human rights and freedom of information.
- Each information asset will have a nominated owner who will be assigned responsibility for defining the appropriate uses of the asset and ensuring that appropriate security measures are in place to protect the asset
- Information will be made available solely to those who have a legitimate need for access.
- All information will be classified according to an appropriate level of security.
- The integrity of information will be maintained.
- It is the responsibility of all individuals who have been granted access to information to handle it appropriately in accordance with its classification.
- Information will be protected against unauthorised access.
- Compliance with the Information Security policy will be enforced.

Governance

Responsibility for the production, maintenance and communication of this top-level policy document and all sub-policy documents lie with the Director of IT Services, Falmouth Exeter Plus and the Registrar, Falmouth University

This top-level policy document has been approved by the CEO and Senior Executive Team (SET) of Falmouth Exeter Plus and the Vice Chancellors Executive Group, Falmouth University. Substantive changes may only be made with the further approval from both these bodies.

Each of the documents constituting the Information Security Policy will be reviewed annually. It is the responsibility of the Director of IT Services and Registrar to ensure that these reviews take place. It is also the responsibility of the Director of IT Services and the Registrar to ensure that the policy set is and remains internally consistent.

Changes or additions to the Information Security Policy may be proposed by any member of staff, via their Director or Department to the Director of IT Services or Registrar.

Any substantive changes made to any of the documents in the set will be communicated to all relevant personnel.

Sub-Policies

Sub-Policy Document List Name	Reference
Business Continuity	ISP002
Compliance	ISP003
Outsourcing and Third Party Compliance	ISP004
Human Resources	ISP005

Information Handling	ISP007
User Management	ISP008
Acceptable Use	ISP009
Access To Sensitive Material	ISP010
System Management	ISP011
Network Management	ISP012
Software Management	ISP013
Mobile and Remote Working	ISP014
Computer Users Agreement	ISP015
Encryption	ISP016
ResNet Acceptable Use	ISP017
Investigation of Computer Use	ISP018
Local Administrative Right	ISP019
PREVENT Monitoring	ISP020