High Level Information Security Policy

Author: Raymond Scott (ITCS)

Date: 5 October 2017

Version: 2.0

This document defines the University's policy on Information Security and is based on the following principles.

- **Maintaining confidentiality, integrity and availability of information.**
- **Handling information appropriately and according to its data classification.**
- **Preventing disruption to work being undertaken within academic, research and support services that lead to financial loss or loss of reputation to the University.**
- **Ensuring business continuity and minimising business damage by managing and minimising the impact of information security incidents.**

Version history

Version	Date	Note
0.1	4 April 2012	Review and conversion of old policy (2004) into new format with minor adjustments
0.2	11 April 2012	Comments added from SPC review
0.3	2 October 2012	Comments added from ISD review
0.4	25 October 2012	Comments added from community review
1.0	8 November 2012	Comments added from ISSC review. Approved by ISSC
1.1	19th August 2013	Changed URL to English version of BSI
1.2	5 October 2017	Reviewed and updated
2.0	20 October 2017	Approved by ISSC

Introduction

The confidentiality, integrity and availability of information are of great importance to the operation and administration of UEA. Failure in any of these areas can result in disruption to the services that UEA provide as well loss in confidence in the University by existing and potential students and organisations investing in University research projects. The security of our information and other assets is therefore regarded as fundamental to the successful operation of the University.

Scope

This policy applies to:

- All students, staff and visitors to the University of East Anglia
- All information assets owned or managed by the University
- Access rights and controls to information
- Security of services and information systems
- Business continuity and disaster recovery of information
- Appropriate controls to meet regulatory and legislative requirements

- Framework for third parties and University staff to adhere to
- Promotion of security and guidance and advice where appropriate
- Processes to deal with security breaches

Aims

The Information Security Policy should provision business continuity and minimise business damage by preventing and managing to an acceptable level the impact of information security incidents.

Adherence to this policy will help to protect the University, our students, customers and staff from information security threats, whether internal or external, deliberate or accidental. We are committed to good information security provision for our students, customers and for our employees.

It is recognised that detailed policies and procedures are required and the University is committed to implementing these in full.

Policy statements

These policy objectives are achieved through the implementation of our Information Security Policy, which includes security standards, procedures and guidelines developed in accordance with ISO27001. It is the University's policy to:

- ensure that information is accessible only to those authorised to have access;
- safeguard the accuracy and completeness of information and processing methods;
- ensure that authorised users have access to information and associated assets when required;
- ensure that information it manages shall be secured to protect against the consequences of breaches of confidentiality, failures of integrity or interruptions to the availability of that information;
- define an information classification scheme describing classes and how information of a particular class should be managed (stored, accessed, transmitted, shared, and disposed of);
- meet all information security requirements under appropriate regulations, legislation, organisation policies and contractual obligations;
- address the security of all of our services and processes to ensure that risks are identified and appropriate controls are implemented and documented;
- provide a secure working environment for staff and contractors at our sites;
- produce business continuity and incident response plans for strategic University IT and information services, which will be maintained and tested on a regular basis;
- require all third parties working on our behalf to ensure that the confidentiality, integrity and availability requirements of all business systems are met;
- promote this policy and raise awareness of information security throughout the University;
- provide appropriate information security training for our staff and students.

Responsibilities

Ultimate responsibility for the execution of this policy rests with the Vice-Chancellor of the University. The Director of IT, assisted by the Assistant Director Strategy, Policy and Compliance, is responsible for the production and maintenance of University Security Policies, the controls to enforce the polices and the provision of advice and guidance on its implementation and maintenance.

All breaches of information security will be reported to the Assistant Director Strategy, Policy and Compliance, and investigated by appropriate staff.

It is the responsibility of all students, staff and visitors to adhere to this policy.

University Deans of Faculty, Heads of Schools and Central Services Directors are responsible for implementing the policy within their areas of responsibility and for ensuring the adherence of their staff to the policy.

The University reserves the right to inspect any data stored on University computer or telecommunication systems, or transmitted or received via the University's networks, in the course of investigating security incidents, or safeguarding against security threats.

Within this policy, the following individuals have the following responsibilities:

Responsibility	**Owner**
Execution of this policy	Vice-Chancellor
Sponsor and Quality Assurance of this policy	ISSC
Production, maintenance, controls and guidance of this policy	Director of IT
Protection of information systems and assurance that security processes and controls have been carried out	Information system owner (Head of Department managing the system)
Initiation, co-ordination and investigation of potential breaches in policy	Assistant Director Strategy, Policy and Compliance
Ensuring staff have an awareness of and put appropriate controls in place to adhere to the policy	Deans of Faculty/Heads of School/ Central Services Directors
Provide advice, guidance, training and support on information security to the University community	Director of IT
Adherence to policy	All students, staff and visitors

References

This Information Security policy is supported within the context of the following pieces of legislation, professional standards, sector best practice guidance, and University documents:

- ISO27001 provides a specification for an information security management system; ISO27002 is a code of practice for information security management https://www.iso.org/isoiec-27001-information-security.html
- BSI IT security baselines https://www.bsi.de
- Information Technology Infrastructure Library (ITIL) is a collection of best practices in IT service management https://www.axelos.com/best-practice-solutions/itil
- Janet security policy https://community.jisc.ac.uk/library/janet-policies/security-policy
- UCISA Information Security Toolkit http://www.ucisa.ac.uk/publications/toolkit.aspx
- ISD Strategy https://portal.uea.ac.uk/information-services/strategy-planning-and-compliance/isd-strategy

Review

This Information Security policy will be reviewed every 24 months or sooner as necessary by the Strategy, Policy and Compliance team to ensure that it remains current in the light of relevant legislation, organisational procedures or contractual obligations. Changes will be agreed with the Director of IT, and authorisation and quality assurance will be provided by the Information Strategy and Services Committee (ISSC).