Information Classification and Data Management policy

Report Control Information

Title:	Information Classification and Data Management Policy
Date:	06 February 2018
Version:	5.0 (Approved by ISSC)
Authors:	ITCS
Quality Assurance:	ISSC
Security class	Open

Revision	Date	Revision Description
v.1.0	17/07/07	As approved by ISSC
v.1.2	09/05/11	Reviewed and approved by ISSC June 2011. Revised by Security Review project and including external consultant recommendations
v.1.3	14/05/11	Updated for review by IT Forum 21/5/12 and ISSC 12/6/12
v.2.0	12/06/12	As approved by ISSC
v.2.2	16/01/15	Reviewed and updated (removed Internal class and renamed Public to Open)
v.3.0	16/02/15	As approved by ISSC
v.3.1	20/04/17	Reviewed and updated (broke down security impact by CIA)
v.4.0	13/06/17	As approved by ISSC
v.4.1	14/11/17	Reviewed and updated (added Confidential-Sensitive class)
v.5.0	30/01/18	As approved by ISSC

Definitions of terms

Information Asset	An information asset is a collection of any type of data, irrespective of type (e.g. numerical data, text) and format (e.g. digital or hard copy).
Data Owner	The Data Owner is the person or department within UEA who acts as the principle authority and has overall responsibility for the information asset and for ensuring that it is managed securely and in compliance with University and government regulations and policies. The Data Owner may delegate day-to-day responsibility for management of the data to a Data Administrator, service group or other persons.
Data Administrator	The Data Administrator is the UEA staff member or department delegated with overall responsibility for day-to-day management of the information asset in accordance with University and government regulations and policies. Processes and procedures used to manage the data should have been agreed with the Data Owner. For some data, particularly small datasets, the Data Owner and Data Administrator may be the same person.

Security class	Defines how an information asset should be handled. The classes are: Open, Confidential, Confidential-Sensitive and Secret. The classification of an information asset may change over time.
Data management plan	A document which describes how you will handle the data associated with a project, both during its lifetime and after it has completed.
Information asset register	A document listing your information assets and key metadata about them: owner, administrator, location, user access, retention policy, and information class.
Data protection legislation	The Data Protection Act 1998 or from the date that it comes into effect in the UK the General Data Protection Regulation (EU) 2016/679 and the Privacy and Electronic Communications (EC Directive) Regulations 2003 and any guidance or codes of practice issued by the Information Commissioner or any other designated Supervisory Authority in the UK from time to time.

Objective

The objective of this policy is to provide a classification system for all University data and documents (**information assets**) to which an appropriate **security class** can be assigned.

The University holds many information assets that must be protected against unauthorized access, disclosure, modification, loss or other misuse. Efficient management of these assets is also necessary in order to comply with legal obligations under Data Protection Legislation, the Freedom of Information Act and Environmental Information Regulations.

Different types of information assets require different security measures. Proper classification is vital to ensuring effective data security and management. Each security class listed in the summary tables below has defined data management controls which determine how information assets should be handled throughout its lifecycle. These controls should be applied to all information assets held by the University.

Scope

This policy is to be applied to all information held by the University, including data and documents relating to UEA teaching, research and administration. The main focus of the policy is on information held in an electronic format, however the policy also requires departments to apply appropriate controls to information held in hard copy. The policy encompasses storage, access, sharing and resilience of information assets.

Responsibility

Data Owners and **Data Administrators** are responsible for identifying the appropriate security class for any information assets within their care and ensuring that the appropriate data management policies governing storage, dissemination, disposal etc. are followed. Where the asset contains personal data, the data owner is also responsible for deciding on and applying appropriate technical and organisational measures required to protect the data from loss, destruction or damage. These measures are reviewed and approved by the Data Protection Officer (DPO).

Where information is classified not for public consumption (i.e. Confidential, Confidential-Sensitive or Secret) this should be made clear to those who have access to the data. If management of such data is delegated to other individuals or third party organisations, the Data Owner and Data Administrator must ensure that appropriate guidance and/or contracts as appropriate are in place.

Data Owners and Administrators are responsible for ensuring that information assets are processed and managed in accordance with UEA's Records Management policies as detailed at:

https://portal.uea.ac.uk/information-services/strategy-planning-and-compliance/regulations-and-policies/information-regulations-and-policies/records-management.

Audit and accountability

All projects and services with significant handling of data should have a documented **data management plan/information asset register** describing the data to be used, the Security Classes assigned to these categories of data, the identity of the data owners and the data management policies to be applied. The plan/register should be made available on request to those authorised by the University to carry out security or data protection audits (contact ITCS information compliance team for details).

With regard to personal data, under GDPR, the University is obliged to maintain records of processing activities. These records are managed by the University's Information Compliance team, in collaboration with individual departments, and will be made available to the Information Commissioner's Office on request.

Implementation

At the point of creation, all University data will be classified and handled in accordance with the following tables of Information Classes and Data Management Policies. By default, all data are classed Open (accessible to the world). One of the other security classes is applied to data which must be protected.

Incident management

Where data has been incorrectly classified, or has not been managed in accordance with its security class, this should be reported immediately to the Information Compliance team who will log the incident and refer it to the service team, Data Administrator or Data Owner as appropriate for them to action.

Review

The policy will be reviewed every two years by the Information Compliance team. Changes will be agreed with the Director of IT, and approval and quality assurance will be provided by the Information Strategy and Services Committee.

Summary tables of Information Classes and Data Management

Security class	OPEN
Description	Public information relating to the University. E.g. programme and course information on UEA's web pages, press releases, published research papers, printed University student prospectus
Storage	Stored on centrally managed facilities backed up on a 24hr basis, e.g. centrally managed filestore, UEA Office 365 OneDrive for Business and UEA web pages including intranet pages[1]. Or Appropriate third party storage
Dissemination, access, and handling	• Widely available • Unrestricted dissemination via electronic or hard copy • Dissemination must not violate any applicable laws or regulations • Information should be identifiable as from UEA • Permissions to modify limited to authorised persons and procedures in place to ensure that information is kept up to date
Transmission or collaboration	Via web, email, UEA Office 365 OneDrive for Business, appropriate third party storage or printed copy
Security impact[2]	Confidentiality: N/A Integrity: Insignificant to minor Availability: Insignificant to minor
Example security measures[3]	• Stored on UEA Content Management System (CMS) and public-facing web pages • Stored on author's centrally managed filestore • Stored on OneDrive for Business • Stored on departmental central filestore share with write permissions restricted to authorised individuals
Disposal	• Electronic data deleted using normal file deletion processes • Printed material disposed of via non-confidential recycled waste, i.e. does not require shredding or disposal in Shredstation bins

[1] You may choose to put Open documents on the intranet if they do not need to be secured, but you want to limit access only to UEA staff and students for some other reason.
[2] The likely impact on the University's business and reputation if appropriate security controls and data management were not applied and unauthorised persons were to gain access to the information, the data were damaged or rendered inaccessible. Impact is described on the following scale: insignificant, minor, moderate, major and catastrophic. Three elements of the security of the data are considered separately: confidentiality, integrity, and availability.
[3] The listed example security measures are not exhaustive and other methods of securing data may be appropriate. Contact infosec@uea.ac.uk for advice.

Security class	CONFIDENTIAL

Description	• Information restricted to members of UEA, partner organisations and other non-University members and individuals, as authorised by Data Owners
	• Information which
	  o is operationally valuable, or
	  o Contains non-sensitive or non-special category personal information, as defined by Data Protection Legislation.
	E.g. records containing small amounts of personal information such as, job offers, confirmation of academic achievements, exam marks, or research data containing non-sensitive personal information, or information which is valuable, but not business-critical or significantly privacy-infringing.

Storage	Stored on centrally managed facilities backed up on a 24hr basis with access restricted to authorised individuals, e.g. centrally managed filestore, UEA Office 365 OneDrive for Business, encrypted device. Hard copy stored in physically secured areas such as locked filing cabinets, offices. Or Appropriate third party storage
Dissemination, access and handling	• Dissemination limited to personnel authorised by the data owner only • Where restricted to a particular group, only authorised personnel allowed to have access to the information

Transmission or collaboration	• May be transmitted within institution systems in unencrypted format
	• May be transmitted outside institution systems in unencrypted format, *only where there is a low risk of harm (e.g. in the event of unauthorised access):*
	  o to the individuals whose data are contained within the material, and
	  o to the University
	When assessing the risk of harm, consideration should be given to the amount of information to be transmitted. Large numbers of records are likely to represent greater risk if made insecure, and should be handled as Confidential–Sensitive, even where the information itself is not highly sensitive
	• Any distributed documents (electronic or paper) to be marked as 'Confidential' and the intended recipients clearly indicated
	• Printed copies to be delivered by hand directly to the recipient. Use of shared folders on centrally managed facilities, for collaboration with external parties use UEA Office 365 OneDrive for Business or a UEA account with VPN access
	• Appropriate 3rd party storage can be used provided encryption /appropriate security controls are in place

Security impact	Confidentiality: Minor to moderate Integrity: Minor to moderate Availability: Minor to moderate
Example security measures	• Security measures will be appropriate to the security impact of data damage or loss • Stored on centrally managed filestore with access control mechanisms applied • Stored on UEA Office 365 OneDrive for Business • In exceptional circumstances where information is stored on portable electronic storage devices or media, that storage to be encrypted • Printed copies kept secure, e.g. in locked filing cabinet with only authorised individuals having access

Disposal	On decommissioning of equipment used to store the data, the storage should be securely wiped to CESG Enhanced standard[4], or physically destroyed. Printed copies to be shredded in a cross-cut shredder.

[4] CESG Enhanced standard - UK Communications Electronics Security Group (CESG) Enhanced standards

Security class	CONFIDENTIAL-SENSITIVE

Description	• Information restricted to members of UEA, partner organisations and other non-University members and individuals, as authorised by Data Owners
	• Information which
	  o is operationally more valuable than Confidential, or
	  o contains sensitive or special category personal information, as defined by Data Protection Legislation, or
	  o consists of a large amount of Confidential information
	E.g. sickness records, financial records, research data containing sensitive personal information, trade union memberships, criminal record data

Storage	Stored on centrally managed facilities backed up on a 24hr basis with access restricted to authorised individuals, e.g. centrally managed filestore, UEA Office 365 OneDrive for Business, encrypted device. Hard copy stored in physically secured areas such as locked filing cabinets, offices. Or Appropriate third party storage
Dissemination, access and handling	• Dissemination limited to personnel authorised by the data owner only • Where restricted to a particular group, only authorised personnel allowed to have access to the information
Transmission or collaboration	• May only be transmitted within institution systems in encrypted format • May only be transmitted outside institution systems in encrypted format • Any distributed documents (electronic or paper) to be marked as 'Confidential-Sensitive' and the intended recipients clearly indicated • Printed copies to be delivered by hand directly to the recipient. Use of shared folders on centrally managed facilities, for collaboration with external parties use UEA Office 365 OneDrive for Business or a UEA account with VPN access • Appropriate 3rd party storage can be used provided encryption /appropriate security controls are in place
Security impact	Confidentiality: Moderate to major Integrity: Moderate to major Availability: Moderate to major
Example security measures	• Security measures will be appropriate to the security impact of data damage or loss • Stored on centrally managed filestore with access control mechanisms applied • Stored on UEA Office 365 OneDrive for Business • In exceptional circumstances where information is stored on portable electronic storage devices or media, that storage to be encrypted • Printed copies kept secure, e.g. in locked filing cabinet with only authorised individuals having access
Disposal	On decommissioning of equipment used to store the data, the storage should be securely wiped to CESG Enhanced standard[5], or physically destroyed. Printed copies to be shredded in a cross-cut shredder.

[5] CESG Enhanced standard - UK Communications Electronics Security Group (CESG) Enhanced standards

Security class	SECRET
Description	Any confidential information which can have a major impact on the long-term viability or interests of the University.
Storage	Stored on centrally provided special facilities or UEA Office 365 OneDrive for Business in an encrypted format. Or Appropriate third party storage
Dissemination, access and handling	Dissemination, access and handling strictly controlled by the Data Owner, limited to very few authorised individuals and all access and handling logged in an auditable manner.
Transmission or collaboration	• Not normally transmitted via email, but where this is essential both the transmission and the content must be encrypted • Shared folders on centrally managed facilities and OneDrive for Business can be used • Appropriate 3rd party storage can be used provided encryption/appropriate security controls are in place. Data owners are advised to seek advice from ITCS in advance of using third party storage for this data class • Where printed, handled according to Committee Office procedures for secret documents
Security impact	Confidentiality: Major to catastrophic Integrity: Major to catastrophic Availability: Major to catastrophic
Example security measures	• The highest level of security control will be applied to Secret information • Stored on special area of central filestore to which only the Data Owner has access and only they can allow access to other authorised individuals • Document access limited at all times by encryption keys • Documents may be distributed only on paper during a meeting to review the information, and collected from all recipients before the meeting closes
Disposal	As for Confidential and Confidential-Sensitive classes. Records of disposal should be created and maintained.