

Information Classification and Data Management policy

Report Control Information

Title:	Information Classification and Data Management Policy
Date:	20 April 2017
Version:	4.0 (Approved by ISSC)
Authors:	ISD SPC
Quality Assurance:	ISSC
Security class	Open

Revision	Date	Revision Description
v.1.0	17/7/07	As approved by ISSC
v.1.2	9/5/11	Reviewed and approved by ISSC June 2011. Revised by Security Review project and including external consultant recommendations
v.1.3	14/5/11	Updated for review by IT Forum 21/5/12 and ISSC 12/6/12
v.2.0	12/6/12	As approved by ISSC
v.2.2	16/1/15	Reviewed and updated (removed Internal class and renamed Public to Open)
v.3.0	16/2/15	As approved by ISSC
v.3.1	20/4/17	Reviewed and updated (broke down security impact by CIA)
v.4.0	13/6/17	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 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.

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, or other misuse. Efficient management of these assets is also necessary in order to comply with legal obligations under the Data Protection Act and the General Data Protection Regulation (GDPR), 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 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://www.uea.ac.uk/is/strategies/infregs/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 ISD SPC for details).

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 Strategy, Policy and 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 Strategy, Policy and Compliance team. Changes will be agreed with the Director of Information Services, 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	<ul style="list-style-type: none"> • 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: Low to medium Availability: Low to medium
Example security measures ³	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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 'blue 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. Three elements of security 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	<ul style="list-style-type: none"> Information restricted to members of UEA, partner organisations and other non-University members and individuals, as authorised by Data Owners Information which is operationally sensitive / valuable or contains personal information relating to individuals. E.g. employee information such as payroll, exam papers, exam marks, notes relating to disciplinary processes, research data containing personal information or information which is of a high value.
Storage	<p>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.</p> <p>Or</p> <p>Appropriate third party storage</p>
Dissemination, access and handling	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> May only be transmitted outside institution systems in encrypted format 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	<p>Confidentiality: Medium to high</p> <p>Integrity: Medium to high</p> <p>Availability: Medium to high</p>
Example security measures	<ul style="list-style-type: none"> 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	<p>On decommissioning of equipment used to store the data, the storage should be securely wiped to CESG Enhanced standard⁴, or physically destroyed. Printed copies to be shredded in a cross-cut shredder.</p>

⁴ 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	<ul style="list-style-type: none"> • 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 ISD 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: Very high to critical Integrity: Very high to critical Availability: Very high to critical
Example security measures	<ul style="list-style-type: none"> • 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 class. Records of disposal should be created and maintained.