SM11.1 Information Classification and Data Management

Note, time has not permitted the usual discussion with the user forums, so discussion is invited at the ISSC meeting.

Summary of main revisions May 2011

General

- Title of policy changed to “Information Classification and Data Management”
- Definitions for Data Owner, Data Administrator etc added

Objective

- Added lead in text to stress importance of classifying and managing data. Also references to DPA and FOI
- Included disposal as one of the key data management tasks in the objectives

Responsibility

- “Data policies” now described as “data management”.
- Text added to clarify responsibilities regarding paper documents produced from electronically stored data.
- Data Owners and Data Administrators now specified as responsible for information classification and application of data management. Also highlighted their responsibility to ensure that guidance is given where elements of data management delegated to others.
- Added link to records management policies.

Incident management

- IT Helpdesk used as reporting point for them to refer to relevant authority

Audit and accountability

- Emphasis now on having a data management plan

Information Classes and Data Management

- Summary table significantly changed:
    - disposal column added,
    - classes reduced to just four: Public, Internal, Confidential, Secret
    - less specific in regards to controls to be applied, giving example etc, but not excluding other possibilities as technology changes.
- More detail added following table giving fuller descriptions etc.

Report Control Information

Title:	Security Manual – SM11.1 Information Classification and Data Management
Date:	9th May 2011
Version:	v1.2 (draft under discussion)
Reference:	ICT/SECMAN/SM11.1/v1.2
Authors:	Steve Mosley
Quality Assurance:	ISSC

SM11.1 Information Classification and Data Management

Scope

The policies detailed here are intended to be applied to all information that is held by the University including data and documents relating to UEA teaching, research and administration. The main focus is on information held, or handled in an electronic format, but top level policies regarding printed copies of data or documents and how these should be disseminated, stored and ultimately disposed of are also included.

Security Control	**Information security classification**.
Objective	The University holds many information assets that must be protected against unauthorized access, disclosure, modification, or other misuse. Efficient management of such assets is also necessary in order to comply with legal and regulatory obligations such as the Data Protection Act, and to ensure efficient handling of Freedom of Information and Environmental Information Regulations requests. Different types of information require different security measures and hence proper classification of information assets is vital to ensuring effective data security and management. The objective of these Information Classification and Data Management policies is to provide a classification system for all University data and documents by which an appropriate security class can be assigned. Each security class has defined data management policies and controls which determine how the data should be stored, handled, disposed of, transmitted and accessed. These policies and controls should be applied to all information assets held by the University including those created prior to the publishing of these policies.
Responsibility	• The Information Strategy and Services Committee (ISSC) are responsible for approving the Information Classification system, associated data management policies and any subsequent changes to these. • Information Services will publicise the classification system and data management policies for electronically stored data. It will provide appropriate IT facilities/mechanisms to facilitate compliance with these. The data management policies will include 'top level' policy regarding publishing and distribution of paper documents produced from electronically stored data, but detailed policies regarding distribution of paper documents are the responsibility of the Data Owner. • Data Owners and Data Administrators[1] are responsible for identifying the appropriate Information Class for any data within their care and ensuring that the appropriate data

[1] See section on definitions for explanation of the terms Data Owner and Data Administrator.

	management policies governing storage, dissemination, disposal etc. are followed. In particular where data is classified not for public consumption (i.e. Internal, Confidential or Secret) this should be clearly articulated to those who have access to such data. If elements of data management are delegated to other individuals, the Data Owner and Data Administrator must ensure that appropriate guidance is documented and provided. • Data Owners and Administrators are responsible for ensuring that data records are processed and managed in accordance with UEA's Records Management policies as detailed at http://www.uea.ac.uk/is/strategies/infregs/recordsmanagement .
Incident management	Where data is discovered to have been incorrectly classified, or not to have been managed in accordance with its Information Class, this should be reported immediately to the IT Helpdesk who will log the incident and refer it to the service team, Data Administrator or Data Owner as appropriate for them to action.
Audit and accountability	All projects and services which require significant handling of data should have a documented data management plan indicating the different categories of data used within the project/service, the Information Classes assigned to these categories of data and the data management policies to be applied[2]. The data management plan should be made available on request to those authorised by the University to carry out security audits.
Implementation	All University data will be classified and handled in accordance with the attached tables of Information Classes and Data Management Policies at the point of creation.

[2] Some initial discussion has been undertaken regarding data management within research projects. As yet proposals regarding Data Management Plans have not been made and such plans would require a defined structure.

Summary table of Information Classes and Data Management

Class	Description	Storage	Dissemination and access	Transmission	Security impact[3]	Example security measures[4]	Disposal
Public	Public information on behalf of the University e.g. programme and course information on UEA's web pages, press releases, published research papers.	Stored on centrally managed facilities backed up on a 24hr basis e.g. centrally managed filestore and UEA web pages.	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.	Via web, email or printed copy.	Negligible	• Stored on UEA Content Management System (CMS) and public-facing web pages. • Stored on author's centrally managed filestore. • Stored on departmental central filestore share with write permissions restricted to authorised individuals.	Electronic data deleted using normal file deletion processes. Printed material disposed of via 'non-confidential' mechanisms i.e. does not require shredding.
Internal	Information restricted to members of UEA, partner organisations and other individuals, as authorised by Data Owners. Not intended for the public, e.g. internal documents, memos, email and course lists. Information may be restricted to a specific subset of the University, for instance committee papers, or workers on a research project.	Stored on centrally managed facilities backed up on a 24hr basis with access restricted to authorised individuals	Dissemination only to UEA members, or organisations and individuals authorised by UEA. Where restricted to a particular group, only authorised personnel allowed to have access to the information. Permissions to modify limited to authorised persons (e.g. author or authoring department).	Via internal email, UEA Intranet, departmental intranet and printed copy.	Low	• Stored on CMS restricted to UEA only access. • Stored on departmental intranet pages with access restricted to members of the department. • Stored on author's central filestore. • Stored on departmental share on central filestore.	As for Public class.

[3] Security impact in this context is 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.

[4] The listed example security measures are not exhaustive and other methods of securing data may be appropriate. If assistance is required regarding the exact measures that should be used, then Information Services should be contacted for advice.

Class	Description	Storage	Dissemination and access	Transmission	Security impact[3]	Example security measures[4]	Disposal
Confidential	Information which is sensitive or contains personal information relating to individuals, e.g. employee information such as payroll, exam marks, notes relating to disciplinary processes, research data containing personal information.	Stored on centrally managed facilities backed up on a 24hr basis with access restricted to authorised individuals.	Dissemination strictly limited to authorised personnel only.	May only be transmitted electronically 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.	Medium to high	• Stored on centrally managed filestore with access control mechanisms applied. • 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.	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.
Secret	Any confidential information which can have a major impact on the long term viability of the University.	Stored on centrally provided special facilities in an encrypted format.	Dissemination and access strictly controlled by the Data Owner, limited to very few authorised individuals and all access logged.	Not normally transmitted via email, but where this is essential both the transmission and the content must be encrypted.	Very high	• 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.	As for Confidential class.

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

Information Classes and Data management in more detail

Public

The Public Information Class includes information produced by the University and primarily intended for public consumption. For example, programme and course information on UEA's website, press releases, published research papers, basically any information that the University is happy for members of the public to read irrespective of whether or not they have any connection or relationship to the University. The majority of this information will be published on UEA's web pages with world read access, but some information may be stored on other centrally provided facilities and be distributed via other routes. The information can be widely distributed via any means, including web, email and printed copy.

Only members of the University who have been authorised by the Data Owner to modify the information and who have successfully authenticated themselves on the UEA domain will be allowed to change the information. Others who wish to incorporate the information into other documents can request permission from the Data Owner to do so. The information should be clearly identifiable as belonging to UEA and the data kept up to date and backed up on a 24hr basis. Unrestricted dissemination via electronic or hard copy is allowed providing no applicable laws or regulations (e.g. copyright and intellectual property rights) are violated.

Internal

The Internal Information Class includes information that is intended for distribution only to members of UEA, partner organisations, or other individuals as authorised by the Data Owner. Such information is not intended for the public. For example, internal documents and papers, memos, internal email and course lists. In some cases, information may be restricted to a specific subset of the University, for instance School only papers, members of committees and those working on a research project. A significant proportion of this information will be published on UEA's intranet to which only UEA members have access. Some information may be stored on departmental intranets. The information can be disseminated to those authorised to view it by any UEA mechanism including UEA intranet, UEA email service and for printed copies via the UEA postal system. **The default class for any unclassified information is Internal**.

The information should be stored on centrally managed facilities backed up on a 24hr basis with read access restricted to authorised individuals as defined above. Only members of the University who have been authorised by the Data Owner to modify the information and who have successfully authenticated themselves on the UEA domain will be allowed to change the information.

Confidential

The Confidential Information Class includes information which is sensitive or contains personal information relating to individuals, for example employee information such as payroll, exam marks, student records, notes relating to disciplinary processes, research data containing personal information. Access to such information must be strictly controlled and only those members of the University who have been authorised by the Data Owner (or delegated authorities) should have access to the information.

The information should be stored on centrally managed filestore which is automatically backed up on a 24hr basis, with access control mechanisms applied which restrict access to authorised individuals who have authenticated via the UEA domain. Only members of the University who have been authorised by the Data Owner to modify the information and who have successfully authenticated themselves on the UEA domain will be allowed to change the information. Where the Confidential data is part of a service such as the Student Information System or Payroll System where access to subsets of data is dependent on the UEA member's role, mechanisms must be in place to ensure that access is restricted to only those parts of the data to which they should have access. Such services should have been implemented in consultation and with the approval of Data Owners.

The information should only be transmitted electronically in an encrypted format in accordance with the University's encryption policies[6]. In exceptional circumstances where information is required to be stored on portable electronic storage devices or media, authority to do so should have been granted by the Data Owner and the storage encrypted.

.On decommissioning of the computer or storage system used to access or store the data, the storage should be securely wiped to CESG Enhanced standard to guarantee the data cannot be recovered or reconstructed. Where this cannot be done the storage should be physically destroyed. It should also be noted that the SAN is used to provide central filestore and storage for services and this uses RAID technology which automatically stores data in multiple fragments across storage disks and repurposes storage as necessary. Measures are in place to ensure that there is negligible risk of users inadvertently or maliciously gaining access to any confidential data either as a whole or in part.

Where printed copies have to be distributed, these should be marked as 'Confidential' and delivered by hand directly to the recipient. Any stored printed copies should be kept secure, for example in a locked filing cabinet with only authorised individuals having access. Printed copies no longer required should be shredded.

Secret

The Secret Information Class includes any confidential information which can have a major impact on the long term viability of the University. This would be information that in general is known to only a few individuals such as the Vice Chancellor, Registrar etc.

As such it is vital that access to such information is strictly restricted to those few individuals who need to be aware and any electronic copies should be stored in an encrypted format on centrally provided special facilities for this class of information. Access permissions to the information should be controlled by the Data Owner and document access limited by encryption keys. Encryption keys should not be transmitted via email, but by other means such as face to face contact or over the phone. All access to the information should be logged.

Dissemination of copies of the information (electronic and paper) should be strictly controlled by the Data Owner, limited to very few authorised individuals. The information would not normally be transmitted via email, but where this is essential both the transmission and the content must be encrypted in accordance with the University's encryption policies and controls (see reference and footnote under Confidential Information Class). On decommissioning of the computer or storage system used to access or store the data, the storage should be securely wiped to CESG Enhanced standard to guarantee the data cannot be recovered or reconstructed. Where this cannot be done the storage should be physically destroyed.

All printed copies of information in this class should be shredded when no longer in use and whilst in use must be stored securely in a locked filing cabinet or similar facility.

Definitions of terms used

Within the context of this policy the following definitions are to be assumed.

Information Asset and Data

Information asset is a collection of any type of data irrespective of type (e.g. numerical data, text) and medium on which it is stored on. It includes electronic (disk or magnetic based storage), paper or other formats (eg. photographic slides).

Data Owner

The Data Owner is the person or department within UEA which has overall executive responsibility for the data and for ensuring that mechanisms have been put in place to ensure that the data is managed in a secure fashion and in compliance with University and government regulations and policies. In many cases the Data Owner will delegate day to day responsibility for management of the data to a Data Administrator, service group and/or other persons. For example, for UEA finance data the Finance division (FIN) is the Data Owner, but day to day management of the data is automated and managed by Corporate Information Services (CIS).

---

[6] See SM21.1 Encryption Policies and Controls at https://intranet.uea.ac.uk/is/itregs/ictpolicies/secman/Encryption+policies+and+controls

Data Administrator

The Data Administrator is the person or department delegated with overall responsibility for day to day management of the data 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.

Data management

Used to refer to how data is stored, handled, access controlled, transmitted and disposed of when no longer required.