ISC11D48

University of East Anglia

Title:	Information Classification and Data Policies – discussion paper for IT Forum 21/05/12
Author:	Jonathan Colam-French
Date:	14/05/2012
Circulation:	*IT Forum, 21 May 2012*
Agenda:	ISC11A003 – A5
Version:	Draft v0.1
Status:	Open

Issue

The Information Classification and Data Management Policy has been revised to reflect changes in technology and the way that these impact working practices. The policy is submitted to the ICT Forum for comment in advance of submission to ISSC for approval.

Recommendation

It is recommended that the ICT Forum endorse this policy.

Resource Implications

None

Equality and Diversity

This policy has no impact on groups with protected characteristics.

Timing of decisions

This policy will be submitted to ISSC for approval on 12 June 2012.

Further Information

Enquiries about the content of the paper should be addressed to Jonathan Colam-French (j.colam@uea.ac.uk) – ext 3858).

Background

Cloud computing and ready access to mobile devices have changed the way that we are working, it is imperative that our security policies take account of these new technologies and continue to provide a mechanism for ensuring security of key information and data. The Information Classification and Data Management Policy is central to this.

ISC11D48

Discussion

SM11.1 Information Classification and Data Management

Report Control Information

Title:	Security Manual – SM11.1 Information Classification and Data Management
Date:	20th July 2011
Version:	v1.2 (Approved by ISSC June 2011)
Reference:	ICT/SECMAN/SM11.1/v1.2
Authors:	Steve Mosley
Quality Assurance:	ISSC

Revision	Date	Revision Description
V1	17/7/07	As approved by ISSC July 2007
V1.2	9/5/11	Reviewed and approved by ISSC June 2011. Revisions as part of Security Review project and based on recommendations following external consultants report.
V1.3	14/5/11	Updated for review by IT Forum 21/5/12 and ISSC 12/6/12

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. The policy considers the aspects of storage, access and sharing, and resilience. A guide to the selection of non-UEA data storage and transfer solution is given in appendix A of this document.

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, where data is stored on third party systems Information Services will provide guidance to support a risk assessment of the storage. • 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 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.

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

[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 or collaboration	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. Or Appropriate 3rd party storage[5]	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, appropriate third part storage 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.

[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.

[5] Guidance on the selection of appropriate third party storage is provided in Appendix A of this document

Class	Description	Storage	Dissemination and access	Transmission or collaboration	Security impact[3]	Example security measures[4]	Disposal
Internal	Information restricted to members of UEA, partner organisations and other individuals, as authorised by Data Owners. Not intended for the general public. Information may be restricted to a specific subset of the University including a restricted set of non-University members. Examples may include, internal documents, memos, course lists, collaborative documents and research data sets of a non confidential nature. .	Stored on centrally managed facilities backed up on a 24hr basis with access restricted to authorised individuals. Or Appropriate 3rd party storage	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, shared folders on centrally managed facilities, appropriate 3rd party storage 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.

Class	Description	Storage	Dissemination and access	Transmission or collaboration	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 or information which is of a high value.	Stored on centrally managed facilities backed up on a 24hr basis with access restricted to authorised individuals. Or Appropriate 3rd party storage	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. Use of shared folders on centrally managed facilities, for collaboration with external parties a UEA account and VPN access can be set up. Appropriate 3rd party storage can be used provided encryption /appropriate security controls are in place	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[6] , or physically destroyed. Printed copies to be shredded.

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

Class	Description	Storage	Dissemination and access	Transmission or collaboration	Security impact[3]	Example security measures[4]	Disposal
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. Or Appropriate 3rd party storage	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. Shared folders on centrally managed facilities 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.	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.

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 default class for any unclassified information is 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 (this may include a restricted subset of members of the public, for example researchers collaborating on a project). Such information is not intended for the public in general. For example, internal documents and papers, memos, internal email, course lists and research data which forms part of a current research project. 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, third party storage and for printed copies via the UEA postal system.

Where information is required to be shared with a subset of the public it is not possible to use all of the dissemination methods, in particular the intranet and shared folders on centrally managed facilities are not available for this purpose. The information should be stored on secure facilities and backed up on a 24hr basis with read access restricted to authorised individuals as defined above. Only people authorised by the Data Owner to modify the information and who have successfully authenticated themselves 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.

Where confidential information needs to be shared electronically it should only be transmitted in encrypted format and should be marked as Confidential. If the information is internal to UEA members only then the information should be stored on centrally managed filestore, with access control mechanisms applied which restrict access to authorised individuals who have authenticated via the UEA domain. Shared folders on UEA centrally managed facilities are available for collaboration and for collaboration with external parties a UEA account and VPN access can be set up.

Third party storage can be used for this class of information provided appropriate security controls are in place, if in doubt data owners are advised to seek advice from ISD.

Only members of the University who have been authorised by the Data Owner to modify the information and who have successfully authenticated 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[7]. 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). Shared folders on UEA centrally managed facilities are available for collaboration and for collaboration with external parties a UEA account and VPN access can be set up.

Third party storage can be used for this class of information provided appropriate security controls are in place and data owners are advised to seek advice from ISD in advance of setting up any such storage.

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).

[7] 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.

ISC11D40 – Appendix A

IT Forum 21 May Document 5

Guide to Selecting non UEA Data Storage/Transfer Solutions

The following document is designed to assist in selecting suitable 3rd party storage solutions when there is a need to share or transfer data outside of UEA. This relates to all data storage not provided by central ISD provided storage solutions. These include systems such as Dropbox, Google Drive and Microsoft SkyDrive.

The information in the guide should be seen as high level advice only and does not replace any requirements as laid down by the UEA Information Classification and Data Management Policy

🟢 Once you have checked that the Information Classification is correct you should be ok to proceed

🟠 Depending on the content of the data further investigation may be required – proceed with caution

❌ You must ensure all the conditions are met before you proceed

⚠ **All UEA data is subject to Freedom of Information (FOIA) even if stored on 3rd party systems (including email)**

⚠ **It is the responsibility of the person storing data or selecting storage to ensure it is appropriate. ISD can provide advice when required.**

⚠ **If 3rd party storage is used as a primary data store then you must ensure suitable backup solutions (typically backed up every 24 hours).**

Useful Links:

UEA Security and Data Policies	http://www.uea.ac.uk/is/strategies
Information Commissioners Office: Data Protection Act	http://www.ico.gov.uk/for_the_public/the_acts.aspx
Register of US Safe Harbour agreements	https://safeharbor.export.gov/list.aspx
Cloud Storage Comparisons	http://www.theverge.com/2012/4/25/2973849/google-drive-terms-privacy-data-skydrive-dropbox-icloud

Common Privacy and Security Information:

Google	http://www.google.com/policies/privacy/
Apple ICloud	http://support.apple.com/kb/HT4865
Dropbox	https://www.dropbox.com/help/category/Security%20and%20Privacy
Microsoft SkyDrive	http://windows.microsoft.com/en-US/windows-live/microsoft-service-agreement

	Public	Internal	Confidential	Secret
Do users need to authenticate to have access to the data?	🟢	❌	❌	❌
		It should be possible to control access to the data on a user by user basis. You should ensure that you can audit who has been given access, and when this has been used. Passwords should be sufficiently complex to prevent unauthorised access. Some services allow public links to be shared to allow for collaboration – these should not be used.		
Does ownership of intellectual property/copyright remain with the UEA?	🟠	❌	❌	❌
	Unless explicitly required ownership of any rights should not be transferred to the host company.	Ownership of any rights should not be transferred		
Is the data stored on more than one system such as being synced to a local drive?	🟢	🟠	🟠	🟠
		Where data is synchronised to other devices then all copies need to adhere to the recommendation for data encryption		
Is the data stored in an encrypted form in all locations?	🟢	🟠	❌	❌
		Ideally data will be stored in an encrypted form to ensure accountability of who is accessing the data	Data should always be stored in an encrypted form	
Is the data stored within the EEA? *Principle 8 of the DPA is concerned with personal data being transferred outside the EEA unless to a country which has an adequate level of protection*	🟢	🟠	🟠	🟠
		The data should be stored on equipment within the EEA – the only exception to this is if the data is stored with a company that is 'Safe Harbour' registered		
Is the company who store the data Safe Harbour registered?	🟢	🟠	🟠	🟠
		The data should be stored on equipment within the EU – the only exception to this is if the data is		
Is the data encrypted when it is sent from the local computer to the storage provider?	🟢	🟠	❌	❌
		Ideally data will be transferred in an encrypted form	Data must be transferred in an encrypted form (encrypted protocols such as SFTP, FTPS, HTTPS, SSL should be in place)	
Are all copies deleted when you delete the data?	🟠	🟠	❌	❌
	Wherever possible it should be possible to delete information You should ensure it is possible to remove illegal/defamatory content immediately (does the supplier have a 'take down' policy?)		All copies of data held on multiple devices must be deletable – some services keep multiple versions and backups – there should be a level of assurance that these are removed also	

ISC11D40 – Appendix A

	Public	Internal	Confidential	Secret
Is data securely wiped to CESG Enhanced standard?	🟢	🟢	❌	❌
			You must ensure all copies of data are securely deleted to CESG Enhanced standard	
Do we have a Data Protection Agreement with the supplier?	🟢	🟠	🟠	❌
		It is advisable that specific Data Protection Agreements with companies with which we share data should address each of the items listed above and clearly articulate how each of them is addressed for the specific purpose that the data is being shared		Relevant DPA or contractual agreements must be in place

Sample Analysis for the use of DROPBOX

Do users need to authenticate to have access to the data?	!	**Maybe** - Dropbox is authenticated, but it is possible to share files via an email link that is not authenticated It is possible to replicate files to other local machines – these must all be authenticated with suitable usernames and passwords if these conditions are to be met.
Does ownership of intellectual property/copyright remain with the UEA?	✓	**Yes** - Dropbox make no claims over copyright or intellectual property
Is the data stored on more than one system such as being synced to a local drive?	!	**Maybe** - Depending on how you use Dropbox it will synchronise data to other locations and keep multiple copies.
Is the data stored in an encrypted form in all locations?	!	**Maybe** - Data stored on Dropbox is encrypted but unless additional encryption of files is put in place it is not possible to guarantee this for locally synchronised files (eg on an IPad if no complex lock code is set the data will be unencrypted, if a complex lock code is set then it will be encrypted)
Is the data stored within the EEA? *Principle 8 of the DPA is concerned with personal data being transferred outside the EEA unless to a country which has an adequate level of protection*	✘	**No** -Dropbox store data outside of the EEA
Is the company who store the data Safe Harbour registered?	✓	**Yes** - At the time of writing Dropbox are US 'Safe Harbour' registered
Is the data encrypted when it is sent from the local computer to the storage provider?	✓	**Yes** - Dropbox use secure protocols (Secure Sockets Layer (SSL) and AES-256 bit encryption)
Are all copies deleted when you delete the data?	✘	**No** - Since Dropbox keeps multiple versions, enables files to undeleted and enables files to synced to local devices it is not possible to guarantee this
Is data securely wiped to CESG Enhanced standard?	✘	**No** - Dropbox make no statement regarding deletion of data. Data may be kept indefinitely depending on your setup
Do we have a Data Protection Agreement with the supplier?	✘	**No** - The UEA has no formal relationship with Dropbox

Conclusion

🟢 You are probably ok to use the service for **Public** information.

🟠 Depending on the content you may be ok to use the service for **Internal** information but care must be taken.

❌ You should not use the service for **Confidential** information.

❌ You should not use the service for **Secret** information.