University of East Anglia

Information Security Classification Scheme

Security class	OPEN	CONFIDENTIAL	CONFIDENTIAL-SENSITIVE	SECRET
Description	Public information relating to the University. Does not contain information: that is operationally sensitive or contains personal data that cannot be made public.	Restricted to members of UEA, partner organisations and other non-University members and individuals, as authorised by information asset/data owners. Information which is operationally valuable, or contains non-sensitive or non-special category personal information, as defined by data protection legislation which cannot be made public.	Restricted to members of UEA, partner organisations and other non-University members and individuals, as authorised by information asset/data owners. Information which is operationally more valuable than Confidential, or contains sensitive or special category personal information, as defined by data protection legislation, or consists of a large amount of Confidential information.	Restricted to members of UEA, partner organisations and other non-University members and individuals, as authorised by information asset/data owners. Any confidential information that can have a major impact on the long-term viability or interests of the University. Information which consists of a large amount of Confidential-sensitive information.

Examples	• programme and course information
	• press releases
	• published research
	• University prospectus
		• personal information such as:
		  ○ job offers
		  ○ confirmation of academic achievements
		  ○ exam marks
		• research data containing non-sensitive personal information, or information which is valuable, but not business-critical or significantly privacy-infringing.
			• sickness records
			• extenuating circumstance data
			• financial records
			• research data containing sensitive personal information
			• trade union memberships
			• criminal record data
				• research data containing material classified by HM Government – or similar bodies - as secret

Risk / compliance impact[1]	Nil to Insignificant	Minor to moderate		Major to catastrophic

[1] 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.

Security class		OPEN	CONFIDENTIAL	CONFIDENTIAL-SENSITIVE	SECRET
Storage & transmission	*Website*	✓	✗	✗	✗
	Intranet (MyUEA)	✓	✗	✗	✗
	Email	✓	✓	✓	✗
	UEA SharePoint (incl. Teams)	✓	✓	✓	✓
	UEA Shared Network Drives	✓	✓	✓	✓
	UEA approved Content Management System	✗	✓	✓	✓
	Third Party Solutions	✓	✓	✓	✓
	Paper	✓	✓	✗	✗
Transmission or collaboration		Unrestricted dissemination via electronic or hard copy	• 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	• 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 • Appropriate 3rd party storage can be used provided encryption /appropriate security controls are in place	• Not normally transmitted via email, but where this is essential both the transmission and the content must be encrypted • Appropriate third-party storage transmission mechanisms can be used provided encryption/appropriate security controls are in place. • Information asset/data owners are advised to seek advice from ITCS in advance of using third-party transmission tools for this data class. • Where printed, handled according to Governance Office procedures for secret documents

Security class	OPEN	CONFIDENTIAL	CONFIDENTIAL-SENSITIVE	SECRET
Example security measures[2]	Stored on departmental central file stores with restricted permissions to edit Stored on departmental dedicated CMS with restricted permissions to edit Permissions to modify limited to authorised persons and procedures in place to ensure that information is kept up to date	• Security measures will be appropriate to the security impact of data damage or loss • restricted to a particular group and/or storage location, only authorised personnel allowed to have access to the information access and editing control mechanisms applied • storage to be encrypted • Printed copies kept secure, e.g. in locked filing cabinet with only authorised individuals having access		• Stored in special areas of central file stores to which only the information asset/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 • Dissemination, access and handling strictly controlled by the information asset/data owner, limited to very few authorised individuals and all access and handling logged in an auditable manner.
Destruction	• 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 via dedicated bins for disposal of confidential material	• On decommissioning of equipment used to store the data, the storage should be securely wiped to CESG Enhanced standard[3], or physically destroyed. • Printed copies to be shredded in a cross-cut shredder or disposed of via dedicated bins for disposal of confidential material. • Records of disposal should be created and maintained.		

[2] The listed example security measures are not exhaustive and other methods of securing data may be appropriate. Contact infosec@uea.ac.uk for advice.

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

Document Control

The Information Security Classification Scheme replaced the former Information Classification Policy; it forms part of the Records Management Policy. This document mirrors the content of the Records Management Policy.

Version History

Version number	Approval date	Approval mechanism	Details of change
1.1	17/06/2010	Information Security Steering Committee	
1.2	17/04/2013	Information Security Steering Committee	
1.3	30/10/2025	Senior Information Risk Owner (SIRO)	