SM21.1 Encryption policies and controls

Summary of main revisions May 2011

General

- ITCS changed to Information Services throughout

Introduction

- Revised to reflect current situation and encrypted email facilities still to be introduced. Also link to Information Classification and Data Management emphasized

Objective

- Revised to emphasize link to Information Classification and Data Management

Responsibility

- Revised to better reflect current situation

Incident management

- Revised to reflect new IT support structure and Helpdesk as central reporting point.

Audit and accountability

- Emphasis now on Information Services

Implementation

General

- SM21.1.1 – linkage to Information Classification and Data Management policies
- SM21.1.2 – inserted “wherever possible” acknowledging that may not be possible depending on type of service and encryption facility used.

Encrypted data channels and protocols

- SM21.1.3 – inserted “wherever possible”
- SM21.1.4 – simplified to focus on UEA provided and approved email service
- SM21.1.6 – inserted “wherever possible”, accepting that not possible with all server to server data feeds.
- SM21.1.7 – revised to acknowledge that may not be able to provide encrypted data channels in countries where encryption not allowed

File encryption

- SM21.1.8 – revised to “at least 128 bit key” and reference to MS Office documents stored with encryption as a footnote
- Old SM21.1.9 referring to encryption facilities on central filestore removed
- New SM21.1.9 – now distinction between laptops/USB storage devices and others (mobile phones) where encryption not always possible

Email encryption and digital signatures

- SM21.1.10 – Inserted “at least 128 bit key” and emphasised facilities provided in the approved staff email service
- SM21.1.11 – simplified and emphasised provided as part of UEA staff email service

Report Control Information

Title:	Security Manual - SM21.1 Encryption policies and controls
Date:	9 June 2011
Version:	v1.2 (for approval by ISSC June 2011)
Reference:	ICT/SECMAN/SM21.1/v1.2 (DRAFT)
Authors:	Steve Mosley
Quality Assurance:	ISSC

Revision	Date	Revision Description
V1.1	19/8/08	As approved by ISSC June 2008
V1.2	24/5/11	Approved by ISSC xxxxx 2011. Revisions as part of Security Review project.

Introductory note

The policies and controls documented here apply to all encryption use within UEA. They cover both the use of encryption by users to protect sensitive or confidential data and also encryption of data channels as may be used for server to server communication or as part of a service provided within the University. The reader is also advised to note the linkage with the University's Information Classification and Data Management policies[1] where criteria are given for assigning data to the 'Confidential' and 'Secret' Information Classes which require encryption of data and other measures in order to prevent unauthorised access.

In order to fully implement the policies and controls detailed here and integrate encryption facilities into UEA IT services there will be significant costs and development effort involved. There is a need to be pragmatic in choice of software and technologies in order to ensure that such facilities are easy to use and the implications for, and impact on, corporate services and processes will also need to be considered. For these reasons not all elements are immediately implementable (e.g. encrypted email) and the additional facilities required to enable implementation of these elements will be developed as part of Security Project work during the 2011/12 academic year.

SM21.1 Encryption policies and controls

Security Control	Controls covering use of encryption
Objective	To ensure that encryption is used in a consistent and manageable manner in accordance with the policies detailed in the UEA General Information Security Policy (GISP), and applied only to Confidential or Secret Information Classes as defined in SM11.1 Information Classification and Data Management.
Responsibility	Information Services will advise on best practice regarding use of encryption and will provide necessary client based facilities for connection to centrally

[1] https://intranet.uea.ac.uk/is/itregs/ictpolicies/secman/SM11.1+Information+Classification+and+Data+Policies

	provided services where encryption of data and communications is required. It is the responsibility of data owners and line managers to ensure their staff use encryption in a responsible fashion in accordance with encryption policies defined in GISP21 of the General Information Security Policy (GISP) and the controls/policies detailed here.
Incident management	Where encryption processes/procedures are suspected to have been compromised, this should be reported immediately via the Helpdesk to the Data Owner or IT support manager as appropriate.
Audit and accountability	Information Services should review any encryption services they provide on a regular basis (at least annually), checking against these policies/controls and recognised best practice, and taking remedial action as appropriate. Outstanding issues and deviation from these controls that are judged to present a significant security risk should be recorded in a Security Risk Log (see Security Manual SM1.1 IT services/systems security risk log).

Implementation	**General** SM21.1.1 University data (including files and emails) should only be encrypted where there is a need to protect sensitive or confidential data against unauthorised access and in accordance with UEA Information Classification and Data Management policies (see Security Manual SM11.1 Information Classes 'Confidential' and 'Secret'). SM21.1.2 Decryption keys should be stored securely and arrangements made wherever possible for managers to access the keys when personnel are absent and lack of access to the data is preventing/hindering pursuance of UEA work. The keys must also be made available to the relevant authorities during any investigation of criminal activity or financial irregularities. See also the General Information Security Policy, GISP21 Encryption use and key material handling. **Encrypted data channels and protocols** SM21.1.3 Where IT account authentication data such as usernames and passwords are transmitted over the network, for instance in order to connect to a service or open a channel for data transfer, that data should be transmitted in an encrypted format wherever possible following best practice and based on strong encryption using at least 128 bit keys. SM21.1.4 University email clients should use secure protocols as provided by University provided and approved secure email services. Where web services are used to access University email, only the secure https protocol should be used (not http). SM21.1.5 Where confidential or sensitive data is being transmitted using web services, the secure https protocol should be used. SM21.1.6 Server to server data feeds should all be encrypted wherever possible. SM21.1.7 Where members of the University are working in countries which ban or impose severe limitations on use of encryption, the University may not be able to provide encrypted data channels and alternative mechanisms may have to be used. In such cases care should still be taken to ensure good data security. **File encryption** SM21.1.8 File encryption used should be based on strong encryption using at least a 128 bit key[2]. SM21.1.9 Sensitive or confidential data should only be stored on mobile devices where it is essential to do so. Storage of such data on portable computers or USB storage devices should always be encrypted. Storage on other mobile devices such as portable phones should be encrypted, or at the least access to the device password protected, wherever possible. **Email encryption and digital signatures** SM21.1.10 Encryption when used should be based on strong encryption using at least a 128 bit key and public and private keys (e.g. the

[2] Note, if Microsoft Office documents are saved with the encryption option selected, this is the default setting.

		PGP and S/MIME models). Information Services will provide facilities for this within the UEA staff email service[3].
	SM21.1.11	Digital certificates used to verify identity of the sender will be provided via the UEA staff email service for both internal and external email communications where required.

[3] Information Services is working to provide such a facility during the 2011/12 academic year as part of the Security Project.