GISP18. Encryption use and key material handling

Date:	5 October 2017
Version:	2.0
Authors:	Raymond Scott
Quality Assurance:	Information Strategy and Services Committee (ISSC)

Version control

Revision	Date	Revision Description
1.0	8/11/12	Approved by ISSC
1.1	5/10/17	Reviewed and updated
2.0	20/10/17	Approved by ISSC

Policy

Security Control	Control of encryption use by staff, students, and visitors.
Objective	• To ensure that encryption is used in a consistent and manageable manner and applied only to Confidential or Secret Information Classes as defined in the Information Classification and Data Management policy. • To ensure the ability to undertake University work is not adversely affected by the use of encryption.
Policy	18.1. Use of encryption to protect University data should be in accordance with the University's policies on information classification. 18.2. Where encryption is used the encryption method used should follow University defined procedures. 18.3. When encryption is used, details of the encryption method and keys should be securely stored and accessible to the user's line manager or supervisor.
Responsibility	• ITCS is responsible for determining and publishing procedures and guidelines for using encryption. • It is an individual's responsibility to ensure that encryption is only used where justified and in accordance with this Policy and the University's information classification policies. • Note, in the course of any criminal investigation involving encrypted data, an individual may be required to give police access to encryption keys used, or to prove that the keys are no longer in their possession. If University owned data is involved, the administrator for that data, or the project manager would normally be responsible for providing access to encryption keys used.
Incident Management	Where encryption procedures and processes have been compromised the incident should be reported to the administrator for the data concerned, or to their line manager.
Audit and accountability	ITCS 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.
Implementation	**General**

	• University data (including files and emails) should only be encrypted where there is a need to protect secret, sensitive or confidential data against unauthorised access and in accordance with the UEA Information Classification and Data Management policy. • 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. **Encrypted data channels and protocols** • 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 following current industry best practice. • 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). • Only secure protocols should be used (TLS, IPSEC, SSH, etc.). Insecure versions or configurations must not be used (SSL or early TLS). • Where confidential or sensitive data is being transmitted using web services, the secure https protocol should be used. • Server to server data feeds should all be encrypted wherever possible. • 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** • File encryption used should be based on strong encryption following current industry best practice[5]. • 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. • Advice on encrypting Microsoft Office documents is provided in the helpsheet available from https://portal.uea.ac.uk/is/online-wiki-helpdesk/-/wiki/Main/How+to+encrypt+a+Microsoft+Office+document • Advice on creating an encrypted archive containing files of any type is available from https://portal.uea.ac.uk/documents/6207125/6857482/Encrypt%2Ba%2Bfile.pdf **Email encryption and digital signatures** • Encryption when used should be based on strong encryption following current industry best practice and public and private keys (e.g. the PGP and S/MIME models). • 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.

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

	End-user messaging technologies • Where secret, sensitive or confidential information is transmitted via end-user messaging technologies such as email, instant messaging, SMS or chat, it must be sent using strong encryption following current industry best practice. • In particular, the PCI-DSS requires that unencrypted Primary Account Numbers (PAN) are not sent via end-user messaging technologies.