UNIVERSITY OF SUSSEX

IT Services

CRYPTOGRAPHY POLICY

1. OVERVIEW AND PURPOSE

1.1 Information has value and access to it must be managed with care to ensure that confidentiality, integrity and availability are maintained.

1.2 Encryption of information and devices helps mitigate the risk of unauthorised disclosure and tampering. It helps to ensure that access to University information is only granted to those with authorisation.

1.3 This policy establishes the requirements for the application of encryption as a means of protecting the University's information assets. It sets out how information should be protected by encryption when it is being accessed, transferred or stored.

1.4 This policy enables the University to manage encryption in a consistent manner and to appropriately safeguard access to all University information assets and avoid breaches of the Data Protection Act 2018 and other statutory, regulatory or contractual obligations.

2. SCOPE

2.1 The policy covers the application of encryption to information processed with University managed information technology services and equipment including those provided by third parties. This includes, but is not limited to:

- University owned laptop and desktop devices
- University owned removable media and mobile devices (e.g. mobile phones, USB sticks, tablets)
- Services used to access information and other services within the University's Network (Network traffic and infrastructure, data centres, VPN, Wi-Fi)
- Wired and wireless networks
- Cloud hosted services

2.2 Collecting, recording, storing, using, analysing, combining, disclosing or deleting data is covered under the terminology of processing.

2.3 This policy applies to information classified sensitive or protected under the University's Information Classification and Handling Policy, including when processed using a personally owned device (see Bring Your Own Device Policy). Information shall be taken to mean both information and data.

2.4 This policy applies to all users including staff, students and associates of the University who process sensitive and protected information on behalf of the University.

2.5 Where valid business reasons exist, exceptions to this policy can be recommended by Heads of Schools/Directors of Professional Services and signed off by the Director of ITS.

3. RESPONSIBILITIES

3.1 Information Governance Committee (IGC)

3.1.1 Responsible for ensuring that the necessary processes and systems are in place to support this policy.

3.1.2 Responsible for ensuring that the policy is regularly reviewed and remains fit for purpose.

3.2 Senior Information Risk Officer (SIRO)

3.2.1 Responsible for ensuring that this policy aligns with the risk appetite of the University, ensuring that risks associated with the information assets are appropriately managed.

3.3 Director of IT Services

3.3.1 Responsible for ensuring that the policy and security of information in the context of the use of information assets aligns with and supports the University's agreed strategic framework for information technology systems. Responsibility of the day-to-day operation may be delegated.

3.3.2 Responsible for ensuring key management procedures related to this policy are in place.

3.3.3 Responsible for ensuring that adequate technical advice and guidance is made available to all users including staff, students and associates of the University regarding the appropriate mechanisms for the processing of information in a secure manner.

3.4 Data Protection Officer (DPO)

3.4.1 Responsible for monitoring compliance with personal data protection requirements and for advising on personal data protection obligations under this policy.

3.4.2 Responsible for maintaining the Information Asset Register.

3.4.3 Responsible for determining the Information Classification and Handling Policy and supporting documentation.

3.4.4 Responsible for ensuring that adequate advice and guidance is made available to all staff, students and associates of the University regarding the classification and handling of personal data.

3.5 **Heads of Schools / Directors of Professional Services Divisions**

3.5.1 Responsible for compliance with this policy in their areas, for ensuring that those acting under this policy (for whom they have management or contractual responsibility) are appropriately trained and made aware of their obligations and for reporting non-compliance via the defined and approved channels.

3.6 **Third Parties**

3.6.1 Where third parties are processing University Information, Heads of Schools/Directors of Professional Services are responsible for ensuring controls equivalent to those applicable to University processed information are in place.

3.7 **All Users**

3.7.1 It is the responsibility of all users to adhere to the Information Security Policies and ensure that relevant devices and information are encrypted when required using approved University methods.

3.7.2 All users are responsible for ensuring that any information security incidents are reported promptly and through the appropriate channel.

4. POLICY

4.1 There are situations in which the University's information assets must be protected by applying encryption. These are described in the University's Information Classification and Handling Policy.

4.2 Encryption must be used to protect information classified as sensitive or protected when stored ('at rest') and when being accessed or moved across any computer network ('in transit'), except behind the corporate firewall. Although exemptions may be granted, they must be carefully assessed against the risk, any compensating controls and must be properly authorised. If a user is in doubt whether encryption is required when processing sensitive or protected information the IT Services Helpdesk can give guidance. If the classification of information is not known it must be treated as sensitive.

4.3 Encryption must be implemented using up-to-date and secure methods and technologies.

4.4 **Information at rest**

All University owned devices or personal devices storing any University information classified as sensitive or protected must have encryption enabled. A common example of encryption at rest is applying disk encryption to a portable storage device being used to store information.

4.5 **Information in transit**

When University information classified as sensitive or protected is sent or shared outside of secure University systems, it must be encrypted in transit. Examples of encryption in transit may include encrypting a file before sending by email or creating a website that uses HTTPS certificates to encrypt the information between the source and end user.

4.6 Encryption must not be used to prevent authorised access to information. Keys, passphrases or other secrets used to open access must be made available through secure means (i.e. Not shared on a public forum like a social media group) to enable the University to recover encrypted information as necessary.

4.7 The University recognises that specific research groups and centres may have enhanced requirements as a result of the information security requirements of their external partners.
4.7.1 The IT Services Cyber Security team will advise on the introduction of enhanced measures for specific groups and will support specific information security services as advertised on the IT Services pages.

4.8 **Breach of Policy**

4.8.1 Where there is a deliberate misconduct or behaviour amounting to wilful breach of this policy, or gross negligence causing a breach of the policy, the matter may be considered under the University's Disciplinary Procedure under Regulation 31.

5. LEGISLATION AND GOOD PRACTICE

5.1.1 The National Cyber Security Centre (NCSC) have issued guidance about cryptography. https://www.ncsc.gov.uk/section/advice-guidance/all-topics?allTopics=true&topics=cryptography&sort=date%2Bdesc

5.1.2 The Payment Card Industry Data Security Standard has requirements regarding cryptography. https://www.pcisecuritystandards.org/pdfs/pci_ssc_quick_guide.pdf

Review / Contacts / References	
Policy title:	Cryptography Policy
Date approved:	16 October 2020
Approving body:	Information Governance Committee
Last review date:	29 June 2018
Revision history:	1.0 16 Feb 2010 1.1 07 Jan 2015 1.2 23 Feb 2015 1.3 03 March 2015 1.4 20 June 2017 1.5 29 June 2018
Next review date:	October 2021
Related internal policies, procedures, guidance:	Information Security Policies Information Security Policy ITS Top 10 Security Tips Data Protection Bring Your Own Device Policy Information Classification and Handling Policy Payment Card Industry Data Security Standard Policy Information Asset Register Regulations of the University
Policy owner:	ITS Services
Lead contact / author:	Suzanne Elmore, Cyber Security Manager