Sheffield Hallam University

Electronic Data Encryption Policy

Issuing Authority: Leon Etherington,
Acting Chief Information Officer,
Information Systems and Technology

Signed: 

Date Effective: March 2016

Review date: February 2018

Version: 2016.2

Electronic Data Encryption Policy

Objective

University policy is that appropriate measures are taken to ensure all confidential, personal and sensitive electronic data is stored and transmitted in a secure manner, adhering to the security standards relevant to the type of data and the system it is held upon. This policy outlines the standards which must be adhered to for the storage of such data on mobile devices and the transmission of data between systems.

Mobile Devices

It is University policy to encrypt all confidential, personal and sensitive data stored onto portable devices, e.g. laptops, CDs, disks, mobile phones, PDA's and USB sticks. All such data will be encrypted to FIPS140-2 or above as appropriate to the level of risk associated with the data.

It is the responsibility of the data user to ensure that any personal data they are using on a portable device, personal, non-university PC or laptop is encrypted, or such data is accessed using secure mechanisms which do not store data on the device.

Communications

It is University policy to encrypt all confidential and sensitive personal data when it is transmitted outside the University's secure wired network. It is the responsibility of the data user to ensure that any confidential, personal and sensitive electronic data they are transmitting is encrypted. All communications must be encrypted to appropriate standards depending on the level of risk associated with the type of data and the systems used.

Third Party Hosted data

No third party storage of University owned or controlled data will be authorised unless it meets the requirements set out in this policy and is agreed by the Director of Information Systems & Technology or their nominee. Data should be held on systems which provide levels of physical and electronic security which are at least comparable to those of Sheffield Hallam University's own facilities and which are appropriate to the type of data and the levels of risk.

University data stored by a third party must be held in a physically secure data centre in a country which has enacted Data Protection legislation or signed up to the Safe Harbour scheme[1]. It must be protected by external firewalls with a standard denial policy. All data transfers between the University and the third party must be encrypted, either by using secure protocols such as HTTPS and FTPS or by using a secure VPN.

Authentication

It is University policy that any mechanism used for authentication to any University system should be encrypted to the appropriate standard depending on the level of risk associated with the individual system being accessed.

Internally hosted data

It is University policy to ensure that where necessary networked and local storage devices e.g. PCs hard drives or networked drives, have appropriate level physical security dependant on the data they contain. Such devices will be encrypted based upon risk assessments related to the data stored on the device.

Encryption Keys

To ensure business continuity and compliance with the seventh data protection principle all encryption keys used to secure University data must be stored centrally by IS&T.

Scope

This policy applies to all staff, students, data processors, partners, suppliers and contractors and other authorised users.

Implementation, guidance and good practice

To support the implementation of this policy the University provides a range of encryption products and services to protect against the loss of personal data. These are set out in the SLS guidance on encryption on the SLS website.

Further details about personal data and data protection are available on the University Secretariat Website

---

[1] Countries which have enacted adequate data protection legislation comprise: 1) The EEA is made up of the 27 member states of the European Union (Austria, Belgium, Bulgaria, Denmark, Finland, France, Germany, Greece, Ireland, Italy, Luxembourg, the Netherlands, Portugal, Spain, Sweden, the UK, Hungary, Poland, Estonia, Malta, Latvia, Lithuania, Romania, Slovenia, Slovakia, Cyprus and the Czech Republic) plus 3 of the 4 member states of the European Free Trade Association (Iceland, Norway and Lichtenstein).

[2] The Information Commissioner has also deemed the following countries/areas as having an adequate level of data protection to allow transfer of personal data without breaching principle 8: Bailiwick of Guernsey (i.e. Guernsey, Alderney and Sark), Argentina, Canada, Switzerland and Isle of Man. Please check with University Secretariat for updates to this list.

Transfers to the United States of America may be made where they are covered by the Safe Harbour scheme: http://www.export.gov/safeharbor/sh_overview.html.