GISP23. Mobile devices

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	Controls to minimise the risk of loss of University information assets when using mobile devices such as laptops, mobile phones, data sticks or removable storage or accessing University systems when off site and located at non-University premises.
Objective	To ensure that security is added to mobile devices to prevent unauthorised access and maintain confidentiality. To ensure that all information systems and assets are assessed as to their suitability for mobile or off site access before such access is granted.
Policy	23.1. Persons who will be doing part or all of their work using dedicated equipment in a fixed location outside the organisation (teleworking) must be authorised to do so by an appropriate authority within the organisation. A risk assessment based on the criticality of the information assets being used and the appropriateness of the proposed teleworking location should be carried out. 23.2. Teleworkers will be provided with appropriate computing and communications equipment and must use only this equipment for teleworking. The equipment provided may only be modified or replaced if this has been authorised. All equipment must be returned at the end of the teleworking arrangement, or when the teleworker leaves the organisation. 23.3. All teleworking agreements must include appropriate measures, based on a risk assessment, to protect the security of information assets. Teleworkers must follow the agreed security procedures at all times. 23.4. All teleworking agreements must include rules on the use of equipment provided for teleworking. Teleworkers must abide by these rules at all times unless specifically authorised. 23.5. Persons accessing information systems remotely to support business activities must be authorised to do so by their line manager or the system owner for the information system (as appropriate). A risk assessment based on the criticality of the information asset being used must be carried out. 23.6. Utmost care must be used when transporting files on removable media (e.g. disks, portable HDs, CD-ROMs and USB flash drives) to ensure that valid files are not overwritten and incorrect or out of date information is not imported. 23.7. The University will publish guidelines for users of mobile computing equipment advising them on how these should be used to conform to the information security policies and other good practices.

Responsibility	• ITCS is responsible for ensuring access to services by mobile devices is secured where possible, or unable to be accessed where no security option is available. • ITCS is responsible for providing guidance on good practice in the use of mobile devices. • Users are responsible for ensuring that their use of mobile devices or remote facilities is in accordance with good practice advice and the information security policies.
Incident Management	Incidents should be reported to the IT Service Desk for further investigation.
Implementation	**Exchange mobile device security** An Exchange Security Policy should be applied to all mobile devices which synchronise with Exchange. The following settings for the policy should be applied: • Mobile device requires passcode • Minimum passcode length = 6 • Number of failed pass-code attempts until device is reset to factory default (formatted) = Maximum available[6] • Time without user input after which passcode must be re-entered (in minutes) = 5 • Enforce passcode history (remembers last 3 passcodes) • Require encryption on the storage card • Enable passcode recovery (user can obtain recovery passcode via OWA). • Enable a remote wipe facility for devices that synchronise to UEA email using ActiveSync. This can be used in the event that a device is lost or stolen and can be activated by the owner of the device through OWA. • In extreme circumstances, a remote wipe of a lost or stolen device can be performed by ITCS but only with the explicit consent of the device owner. **Guidelines on use of mobile devices** Guidance on setting up security on a mobile device (phone or tablet) accessing the University email service is available from the ITCS web site at: https://portal.uea.ac.uk/documents/6207125/7752191/11.+Mobile+Device+Security-v1.pdf/

[6] Maximum no. of failed attempts available = 16