Contents

1 Overview

Mobile devices are convenient and useful, but they may expose company's information to unauthorized disclosure due to the fact that they often lack adequate security measures. For example, widespread use of wireless capabilities radically change the way these mobile devices should be used.

Encrypted communications for these wireless transmissions and other security controls are available, but many users may not choose to use these security controls.

2 Purpose

The purpose of this policy is both to protect the confidentiality of any data that may be stored on the mobile device and to protect the company networks from being infected by any hostile software when the mobile device returns within the company's premises or is connected to any company's resources.

3 Scope

This policy and related information security documents apply to all Stanmore employees, consultants and contractors involved within the Stanmore ISMS and PIMS framework. This policy covers any mobile devices brought into Stanmore premises or connected to the organizational network using any connection method (e.g. teleworking). This includes but is not limited to laptops, handheld devices, memory sticks, USB drives, personal digital assistants, and smart phones.

The guidance and standards outlined below are designed to ensure that the information and equipment belonging to Stanmore that is used outside the office environment is afforded similar levels of protection as that equipment and information that is used exclusively within the office environment. This also extends to information processed within a member of staff's home.

4 Policy

4.1 General Points

- Users must take good care of all the equipment in their care to prevent accidental damage, e.g. from rough handling, accidentally spilling drinks on the equipment, or being in close proximity to a heat source;
- Users must not install any software without prior authorisation of his/her head of department who shall consult ICT who maintains a standard list of licensed software and current updates to it;
- Users who tamper with the standard hardware and software configurations on the equipment in their care could face disciplinary action and have the equipment withdrawn;
- Users must not disable any element of the standard configuration for its group of users, including data encryption, screen-saver password and anti-virus software;
- Passwords will be managed in accordance with the Password Security Policy;

- All external email, software or documents will be checked for viruses automatically by using antivirus software which is a part of regular Stanmore environment;
- Valuable information will be backed up to secure storage in line with company policy.

4.2 Mandatory controls:

- An asset register of equipment in use with details of owners and a software register of installed software will be maintained by ICT;
- All third party software installed will be licensed for such usage – obtaining licenses is ICT responsibility;
- Apply antivirus software and updates to all devices;
- Standard configurations will be maintained, updated and applied to individual equipment to provide up-to-date protection features to secure local information -there might be more than one standard configuration, for different groups of users – finance, development, support, etc.

4.3 On the Move (Users)

- Ensure that devices are not left unattended when travelling, being particularly vigilant on public transport and in public places such as stations, airports, pubs and hotels. At other times make sure it is left in a secure place when not in use. For this purpose Stanmore offices are regarded as secure place.
- Whenever practical removable disks should be carried separately. If using a security token to permit authenticated access to a particular device, then the token must be carried separately from the device in question.
- If one has to use a mobile device in a public place, one has to ensure that others cannot see the data, and one should never process confidential material under these circumstances.

4.4 Using Mobile Device Securely (Users)

- If equipment is used to communicate by email or fax information must be transmitted in accordance with Stanmore security procedures.
- Anti-virus software (with regular updates) must be installed on all capable devices.
- Laptops and PDA,s should be fully powered down when not in use (not just suspended), as material may be still in memory.
- Hand-held devices cannot be guaranteed to provide safe storage of information. In the event that a hand-held device is damaged, destroyed, lost or stolen it must be accepted that the information stored on the device will be lost. It is therefore important that critical information held on such a device is stored on a removable medium such as optical disks via

computer/removable disks whenever possible.

4.5 Taking Equipment Abroad

- Before taking a laptop abroad you should seek advice from the Information Security Management Representative or applicable supervisor.
- Some countries prohibit the import, use and/or re-export of certain security devices e.g. encryption. If your PC has such a device and you intend taking it abroad please seek advice on this. The Foreign Office maintains a Web site with this information
- You should be aware that there is an increased risk of equipment being stolen when abroad, and be particularly vigilant at airports when hand luggage is being X-rayed.

4.6 If Equipment in Your Care is Lost or Stolen

Ask colleagues if they have borrowed or moved the missing device. If they have not, then you must report the incident immediately to the Information Security Management Representative.

5 Enforcement

Periodic review of Information Security and personal information management as well as Internal Audits will be the principal entities to periodically measure and report on security and audit controls and therefore ensure that solutions and services are designed, implemented and operated in compliance with this policy and related information security documents. Any employee found to have knowingly violated this policy may be subject to disciplinary action, up to and including termination of employment.

6 Definitions

Asset

Resource, product, process, network element, system component, data or any ISMS entity that can be linked to business objectives or that could have a measurable impact on the organization it were lost.

Control

A security control, also called countermeasures or safeguards, is a mechanism to mitigate, prevent or eliminate a potential risk. An audit control is any control that creates a measurable audit trail or log as well as assists in meeting an audit objective.

System

A system is any collection of processes and/or devices that accomplishes a business objective.

Signed:

Dated: 15/11/19