Strength & Conditioning Education

Guidelines

Remote Access and Mobile Working

1 Introduction

These guidelines aim to outline user responsibility with regards to any remote access systems provided by SCE, and when working with SCE information using mobile devices.

1.1 Purpose

The primary purposes of these guidelines are to:

1. Ensure all users are aware of their responsibilities when working remotely or on mobile devices and understand the associated risks.
2. Provide Remote Access and Mobile Working Guidelines in line with SCE's *Standard - Information Security Classification*.
3. Ensure that all users understand their own responsibilities for protecting the confidentiality, integrity and availability of the data that they handle remotely.
4. Protect SCE from liability or damage through the misuse of its IT facilities.

1.2 Scope

These guidelines apply to all authorised users and the data/ information held, processed or controlled by or on behalf of SCE.

They concern the end use of information used remotely and / or on mobile devices and does not cover the technical security provision of the systems that provide access to information.

SCE does not make provision for all its IT systems and services to be made available remotely. Where the need for confidentiality or integrity of data is extremely high, such as when handling data classified as 'Confidential', remote access will be explicitly denied on request of the data owner, or as contractually demanded.

Users should be aware that the availability and speed of remote access is subject to a number of external factors beyond SCE's control, such as the effectiveness of any Internet Service Provider leased line, or any third party supplied router, firewall, or anti-virus software in being able to create and maintain a connection to SCE systems and services.

1.3 Definitions

Remote Access: accessing SCE systems from outside of SCE premises with an SCE owned, privately owned or publicly accessible computer, laptop, smart phone or other device. The information accessed and processed continues to reside on SCE systems.

Mobile Working - carrying out work (i.e. the creation, storage, processing and transport or transfer of data/ information) as an employee of SCE from outside of SCE premises.

2 Guidelines

2.1 Principles guiding use of remote services and mobile devices

The following principles underpin all considerations of remote and mobile working, and should be considered by all users prior to accessing data remotely:

1. Confidentiality – how will access to your information be restricted to the appropriate people?
2. Integrity – how will information be kept in such a way as to ensure its accuracy, and that it is only changed by the appropriate people?
3. Availability – how will information be available to all who need to access it?

2.2 Information Assessment

The primary considerations for all members of the SCE community when either using remote access services, or working from a mobile device, are:

1. Know what data / information you are using
2. Consider what level of data classification should or does apply to it (for more information please refer to SCE's *Standard – Information Security Classification*)
3. Understand and act upon any particular contractual, ethical or other requirement attached to the information
4. Consider how the mobile devices and the information you are processing can be managed in accordance with their information classification, or if they can't, how you can explicitly accept and manage the risk.

If, after you assess your information, you are not comfortable with the conditions your information is held in, or how it can be accessed remotely, please talk to the Data Protection Officer (DPO) about any steps that can be taken to improve the situation.

2.3 Remote and mobile working with 'Confidential' information

It is important that people accessing 'Confidential' data remotely or on mobile devices clearly assess the risks they are exposing these data and the systems storing them to and consider appropriate steps to keep these secure.

When using remote or mobile devices to process or access data classed as 'Confidential' under, the following minimum standards must be applied:

1. All appropriate system updates have been applied to the device (e.g. Windows updates, iOS updates, application updates)
2. Where appropriate to the device, software firewalls, Anti-Virus software and anti-spyware tools are installed and regularly updated
    1. SCE offers Sophos for free to all SCE staff and Sub-contractors;
    2. free anti-virus tools are available for Windows, Apple Mac and Android devices,
    3. anti-virus products are not currently available for iPhones and iPads
3. Access to the device is controlled by either:
    1. username / complex password meeting SCE's *password requirements* a fingerprint or other biometric access measure,
    2. a complex passphrase that meets the requirements of an SCE user account password (see SCE *password requirements*)
4. The screens of any devices should regularly lock after *a maximum* of 5 minutes' inactivity, requiring re-authentication
5. These data are not accessed from, processed on or stored on public machines (e.g. machines in internet cafes or other public spaces) or via unsecure wired or wireless networks

Additionally, if you are processing 'Confidential' data on a mobile device (rather than just accessing it remotely) you must implement the following steps:

1. The hard drive or storage area of the device is encrypted
2. Any external storage devices are also encrypted
3. If the data are going to be sent to / from the device, they are encrypted before transit (see LSE's *Encryption Guidelines* for further information)
4. Important data is regularly backed up

Please be aware that if you are travelling abroad with a laptop that has an encrypted drive or that contains encrypted data, you may be required by the authorities of that country to decrypt the data or hand over the encryption keys.

Additionally, if the encryption software you are using is not a mass market product freely available to the public, you may need to obtain a Cryptography Open General Export Licence (OGEL) before travelling abroad with it. This will not be the case if you are using any of the products included in our Encryption Guidelines. See the UK Government's note on the export of Cryptographic items at https://www.gov.uk/export-of-cryptographic-items and for more information about OGEL rules https://www.gov.uk/dual-use-open-general-export-licences-explained.

2.4 Remote and mobile working with 'Restricted' information

'Restricted' information would not expose SCE to significant censure or reputational damage were it lost, hacked or leaked. It may however, lead to negative publicity and censure. A series of measures are therefore still recommended in order to mitigate the risks:

1. All appropriate system updates have been applied to the device (e.g. Windows updates, iOS updates, application updates)
2. Where appropriate to the device, Anti-Virus and anti-spyware tools are installed and regularly updated (free anti-virus tools are available for Windows, Apple Mac and Android devices, but are not currently available for iPhones and iPads)
3. Access to the device is controlled by username / password, a fingerprint or other biometric access measure, or a complex passphrase that meets the requirements of an SCE user account password (see the web page on SCE's *password requirements*)
4. The screens of any devices should regularly lock after periods of inactivity, requiring re-authentication
5. These data are not accessed from, processed on or stored on public machines (e.g. machines in internet cafes or other public spaces)

2.5 Remote and mobile working with 'Internal Use' information

1. All appropriate system updates have been applied to the device (e.g. Windows updates, iOS updates, application updates)
2. Where appropriate to the device, Anti-Virus and anti-spyware tools are installed and regularly updated (free anti-virus tools are available for Windows, Apple Mac and Android devices, but are not currently available for iPhones and iPads)
3. Access to the device is controlled by username / password, or in the case of tablets / smartphones, a passphrase or PIN

2.6 Remote and Mobile working with 'Public' information

There are no restrictions on working with 'Public' information.

2.7 Device Theft and information Breaches

Please report the theft of any device holding ‘Confidential’ or ‘Restricted’ information, or any loss of or suspected inappropriate access to ‘Confidential’ or ‘Restricted’ information, to the Incident Response Team. Under the GDPR, SCE has a duty to report a data breach within 72hrs.

2.8 Policy Awareness and Disciplinary Procedures

The loss or breach of confidentiality of personal data is an infringement of the Data Protection Act 1998 and the General Data Protection Regulation and may result in criminal or civil action against SCE.

The loss or breach of confidentiality of contractually assured information may result in the loss of business, financial penalties or criminal or civil action against SCE.

Therefore, it is crucial that all users of the SCE’s information systems adhere to the *Information Security Policy* and its supporting policies as well as the *Standard - Information Security Classification* and the *Data Protection Policy*.

Any security breach will be handled in accordance with all relevant SCE policies.

2.9 Further Policies, Codes of Practice, Procedures and Guidelines

These guidelines sit beneath SCE’s overarching *Information Security Policy*. Other supporting policies have been developed to strengthen and reinforce these guidelines. These, along with associated codes of practice, procedures and guidelines are published together and are available for viewing on SCE’s website. All staff, students and any third parties authorised to access SCE’s network or computing facilities are required to familiarise themselves with these supporting documents and to adhere to them in the working environment.

2.10 Review and Development

These guidelines shall be reviewed and updated regularly to ensure that they remain appropriate in the light of any relevant changes to the law, organisational policies or contractual obligations by the GDPR Readiness Team (GRT).

Additional regulations may be created to cover specific areas.

GRT comprises representatives from all relevant parts of the organisation. It shall oversee the creation of information security and subsidiary policies.

The Data Protection Officer (DPO) will determine the appropriate levels of security measures applied to all new information systems.

3 Responsibilities

Members of SCE:

- All members of SCE, SCE associates, agency staff working for SCE, third parties and collaborators on SCE projects will be users of SCE information, and, may therefore be able to use information remotely or using mobile devices.
- This carries with it the responsibility to abide by the *Information Security Policy*, and its principles and any relevant legislation, supporting policies, procedures and guidance.
- No individual should be able to access information to which they do not have a legitimate access right.
- Notwithstanding systems in place to prevent this, no individual should knowingly contravene this policy, nor allow others to do so.
- It also carries the responsibility to assess the risk to information and handle it appropriately.

Data Owners / Processors:

- Data owners and processors have responsibility for ensuring that appropriate information can be accessed remotely and that, if necessary, additional safeguards to the access of data are requested from Data Protection Officer
- Data owners and guardians include: Directors & Heads of Departments

Data Protection Officer

- Responsible for SCE's compliance with the Data Protection Act and the General Data Protection Regulation.
- Breach reporting to ICO