1. Introduction

1.1. This information security policy document sets out high level principles and expectations that apply to teleworking. It is a sub-document of Information Security Policy (ISP-S1).

1.2. Definitions:

- Teleworking - Article 2 of the European Framework Agreement on Telework of 2002 defines Teleworking as: “a form of organising and / or performing work, using information technology, in the context of an employment contract / relationship, where work, which could also be performed at the employer’s premises, is carried out away from those premises on a regular basis.” (Note: Teleworking can encompass a variety of working arrangements, including home-working, telecentres and working from satellite offices in different locations. Teleworkers may be University employees or self-employed.)

1.3. This document includes statements on:

- Teleworking security policy scope and purpose.
- Authorisation for teleworking.
- Provision of teleworking equipment.
- Security of information while teleworking.

2. Teleworking security policy scope and purpose

2.1. This policy relates to any arrangement where particular staff work at an offsite location, on a regular or long term basis, and which also involves them in:

- Holding significant quantities of confidential University information offsite, whether in electronic or paper format
- Or having a type or level of remote access to information or applications on University servers which exceeds that which is ordinarily available to all staff.

2.2. The purpose of this policy is to ensure that teleworking is undertaken safely from an information security perspective. It is therefore required that information security risks, related to each specific teleworking scheme, are identified assessed and managed.

2.3. These other information security policies are particularly relevant to users of mobile computing devices and those handling confidential information outside secure University locations. They may also therefore be particularly relevant for teleworkers:

- Information Handling Policy (ISP-S7)
- Mobile Computing Policy (ISP-S14)
- Cryptography Policy (ISP-S16)
3. **Authorisation for teleworking**

3.1. Only if the University wishes, and is able, to provide suitable teleworking facilities, may a member of staff undertake teleworking and only in cases where:

- It is the University that requires the member of staff to undertake teleworking or it has been approved for the member of staff to adopt a formal flexible working arrangement. (Note: Staff also applying to adopt formal flexible working arrangements are subject to the University policy on flexible working which is managed by the Human Resources Division.)

3.2. Staff must also be authorised by their Head of Department to undertake teleworking as distinct from other remote working arrangements. This authorisation must be recorded by the department.

3.3. The teleworking authorisation process should involve an assessment of information security risk taking into account several factors: criticality of the information assets being accessed, confidentiality of information being handled and suitability of the teleworking technology and location.

3.4. Those providing or supporting remote access facilities must do so in cooperation and with approval of IT Services. See also:

- Network Management Policy (ISP-S12)

4. **Provision of teleworking equipment**

4.1. Arrangements must be in place to ensure that any University teleworking solutions that should be provided are fully supported and maintained.

4.2. Those responsible for managing provision of teleworking equipment must ensure, on termination of the arrangement, the secure return or disposal of all equipment and information, in electronic and paper form, held by the teleworker.

4.3. Procedures relating to correct usage of any teleworking solution provided must be documented and explained to teleworking staff. In particular the solution must support adequate data backup and teleworkers must understand the backup procedure.

4.4. Any software used as part of a University teleworking solution must be appropriately licensed.

4.5. Any teleworking equipment which provides remote access to the University network, and the authentication method that it uses to access University resources, must be approved by the Customer Service Operations team in IT Services.

4.6. Those responsible for managing provision of teleworking equipment should be mindful that teleworking systems will use an external Internet service provider. It cannot be assumed that behind the scenes technical security measures will be the same as those implemented to help protect campus network devices and this must be reflected when providing appropriate equipment and support.

4.7. Provision and support of teleworking must reliably implement comprehensive information security measures. For details see “Management of mobile computing devices” section in:

- Mobile Computing Policy (ISP-S14)
4.8. Where it is unavoidable that a teleworker must handle confidential information they must be provided with a computer incorporating full disk encryption and where necessary file encryption tools. See:

- Cryptography Policy (ISP-S16)

5. Security of information while teleworking

5.1. Staff, provided with computing and communications equipment for teleworking specifically to protect the security of confidential information, must not put the information at risk by using other less secure equipment.

5.2. Teleworking equipment provided by the University may only be modified or replaced if that has been authorised.

5.3. Teleworking equipment supplied by the University is only to be used by University staff, particularly since others are not bound by University agreements and policies.

5.4. Teleworking staff must ensure that adequate backup procedures for any information held offsite are implemented. It would normally, however, be preferable to remotely access data that is held onsite and already subject to routine backup.

5.5. Only when unavoidable should staff take, send or print hardcopies of confidential documents out of secure University locations. Where absolutely necessary to handle confidential hardcopy documents they should be kept in locked cabinets when not attended (clear desk policy), sent by special delivery post, delivered by hand where possible and disposed of by shredding.

---

**Failure to comply with University Policy may lead to disciplinary action.**

The official version of this document will be maintained on-line. Before referring to any printed copies please ensure that they are up-to-date.