Mobile and Remote Working Policy
Version 2.3
12 December 2012

© University of Leeds 2012
The intellectual property contained within this publication is the property of the University of Leeds. This publication (including its text and illustrations) is protected by copyright. Any unauthorised projection, editing, copying, reselling, rental or distribution of the whole or part of this publication in whatever form (including electronic and magnetic forms) is prohibited. [Any breach of this prohibition may render you liable to both civil proceedings and criminal penalties].
Mobile and Remote Working Policy

Information Security Management

2.3 (12/12/12)

Page 2 of 20

Owner: Kevin Darley, IT Security Co-ordinator, Information Systems Services, University of Leeds

Source Location: M:\Policy\Issued\Copy of Mobile & Remote Working Policy.doc

Document Reference:

Other Documents Referenced:

Related Documents: Information Security Policy

Acknowledgements: Nigel Bruce, Mike Preston and Adrian Ellison for kind production of Annexes C to E Respectively.

Document Control

This document is subject to change control and any amendments will be recorded below.

Change History

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Circulation</th>
<th>Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>08/11/04</td>
<td><a href="http://campus.leeds.ac.uk/isms">http://campus.leeds.ac.uk/isms</a></td>
<td>First formal issue</td>
</tr>
<tr>
<td>2.0</td>
<td>09/11/05</td>
<td><a href="http://campus.leeds.ac.uk/isms">http://campus.leeds.ac.uk/isms</a></td>
<td>Structural changes in line with new standard</td>
</tr>
<tr>
<td>2.1</td>
<td>08/12/06</td>
<td><a href="http://campus.leeds.ac.uk/isms">http://campus.leeds.ac.uk/isms</a></td>
<td>Annual review + alignment with Citrix introduction</td>
</tr>
<tr>
<td>2.2</td>
<td>08/04/08</td>
<td><a href="http://campus.leeds.ac.uk/isms">http://campus.leeds.ac.uk/isms</a></td>
<td>Minor changes throughout and update to Annex A.</td>
</tr>
<tr>
<td>2.3</td>
<td>12/12/12</td>
<td><a href="http://www.leeds.ac.uk/informationsecurity">http://www.leeds.ac.uk/informationsecurity</a></td>
<td>Replace RMAS with Desktop Anywhere</td>
</tr>
</tbody>
</table>

Version Awareness

The audience of this document should be aware that a physical copy may not be the latest available version. The latest version, which supersedes all previous versions, is available at http://www.leeds.ac.uk/informationsecurity. Those to whom this Policy applies are responsible for familiarising themselves periodically with the latest version and for complying with Policy requirements at all times.
Contents

1. Introduction ..............................................................................................................................................4
  1.1. Background ........................................................................................................................................4
  1.2. Purpose, Applicability and Scope ........................................................................................................4

  2.1. Requirement for Policy ........................................................................................................................5
  2.2. Affiliated Supporting Policies ..............................................................................................................6
  2.3. Data Protection Code of Practice ........................................................................................................6

  3.1. The Desktop Anywhere Service ...........................................................................................................7
  3.2. The Creation and Storage of University Data on Privately-owned Computers ...............................8
  3.3. Data Protection Implications - Remote Working Overseas .................................................................8
  3.4. Mobile Workers’ Responsibilities .......................................................................................................9
  3.5. Duty of Care .......................................................................................................................................9
  3.6. Network Connectivity ........................................................................................................................10
  3.7. Data Backup ......................................................................................................................................10
  3.8. Security of Privately Owned Computers and the Protection of Data ...............................................10
  3.9. Incident Reporting .............................................................................................................................11

4. Annexes ..................................................................................................................................................12
  4.3. Annex C – Linux Security Maintenance ............................................................................................16
1. Introduction

1.1. Background

The ever increasing use of digitised and networked information at the University intensifies the risk of data being copied or stolen, or modified, hidden, encrypted or destroyed. Although technical controls provide an essential element of protection, these only deliver a percentage of the required protection, the most effective defence being achieved through awareness and good working practices.

Portable computers that are used for mobile working, and home computers that are used to remotely access to University computing resources, have to be managed effectively in order to minimise the risk that certain information will be denied, lost or compromised, or that staff using such devices will inadvertently fall foul of the law.

This document forms the University’s Mobile and Remote Working Policy in support of the Information Security Policy. Compliance with this Policy will minimise risk to information that is being compiled, used, transported or held outside University premises, where security provision may be lower and exposure to risk may be greater.

The University’s Information Security Policy and a full list of Supporting Policies within the Information Security Management System (ISMS) framework can be found at http://www.leeds.ac.uk/informationsecurity.

1.2. Purpose, Applicability and Scope

This Policy is not intended to create an obstacle to mobile and remote working, and not is intended to support or advocate working from home. Its purpose is to provide controls in respect of remote access to the University’s information assets to protect both individuals and the University from the consequences of accidental disclosure or loss of such information.

This Policy is primarily directed at:

- Staff who use either privately owned or University owned portable computers, such as laptop and tablet computers, personal digital assistants (PDA) and mobile phones with computing and storage capabilities (hereafter referred to as portable computers) to participate in mobile working;
- those who access University systems from home or other remote locations using either privately owned, third-party-owned or University owned equipment; and,
- ISS and faculty/departmental IT support staff who are responsible for systems that are accessed by users remotely.

Relevant requirements naturally extend to anyone else who is subjected to the Policy framework who undertakes activities governed by this Policy.
It is the personal responsibility of each person to whom this Policy applies to adhere fully with its requirements. However, Deans and Heads of Schools/Services are responsible for implementing this Policy within their respective faculty, school or department and for overseeing compliance by staff under their direction or supervision.

Whilst it is recognised that compliance with all aspects of this policy cannot be ‘policed’, those to whom it applies will be held to account for any aspect of non-compliance involving them that subsequently comes to light.

2. Mobile and Remote Working Security

2.1. Requirement for Policy

University information that is held or processed on systems outside of University premises is generally more exposed to being compromised, corrupted or lost than information that is held or processes on systems within University premises. This is down to various factors, such as:

- Laptop computers may be stolen, lost or left on public transport;
- when used in public, data displayed on laptop computers may be subjected to viewing by unauthorised persons;
- physical security in the home may be lower than that of University premises, and some domestic properties may be more prone to burglary resulting in the theft of laptops and private computers;
- data can remain on mobile or remote systems after accessing University systems without some users being aware (i.e. cached web pages and e-mail attachments);
- the University has no jurisdiction over privately owned equipment and when this has been used to access University information, data may be available to be viewed by unauthorised persons;
- the security of machines outside University premises, in terms of security patching and virus protection, may be lower than those within the University and exposure to hacking attacks and virus contamination may be higher;
- unserviceable privately owned equipment containing University data is likely to be repaired through commercial arrangements where data may be viewed by repair staff during that process.

In many cases the disclosure of University information would result in no impact, and the corruption or loss of University data will be little more than inconvenient or cause minor disruption.

However, some University information, such as personal data is sensitive and subjected to legislative control. The unauthorised disclosure, modification or loss of this type of information could result in the prosecution of individuals for breach of the Data Protection Act 1998 if it was found that the data had not been protected and managed in accordance with the requirements of The Act.

* Also generically infers Heads of Centres and Institutes throughout.
Likewise, some finance and research information may be sensitive. Certain research information may be the subject of a non-disclosure agreement imposed by the sponsor. If data of this nature was disclosed it could result in embarrassment to the University and the sponsor, potentially resulting in litigation and a loss confidence which could adversely affect future research grants.

To discharge its duty of care and to protect the interests of its staff, the University has produced this Policy to raise awareness of the responsibilities of those undertaking mobile or remote working activities, and to define the controls required to minimise exposure to sensitive or critical University information.

2.2. Affiliated Supporting Policies

There are various additional Supporting Policies* that have a bearing on mobile and remote working. Of particular relevance are the:

- **Use of Computer Systems Policy** concerning activities which are and which are not permitted using University computer resources and relating to the registration of privately-owned portable computers connected to the University network;

- **Security Patching Policy** concerning the security status currency of computers that access the University’s computer network and resources;

- **Virus Protection & Management Policy** concerning the currency of anti-virus controls and procedures in the event of actual or suspected virus contamination;

- **Information Protection Policy** defining what constitutes both sensitive and critical information and the control requirements for protecting it;

- **Security Incident & Computer Misuse Policy** concerning the reporting and investigation of lost University-owned portable computers, or the compromise of sensitive information or the loss of critical information;

- **Cryptographic Control Policy** concerning the use of encryption software on University-owned portable computers;

- **Systems Security & Network Access & Management Policy** concerning the connection of portable computers to the University Network; and,

- **Data Backup & Storage Policy** concerning responsibilities for keeping portable computers’ data backed-up.

Those participating in mobile and remote working practices are required to familiarise themselves with the relevant aspects of these Supporting Policies and are to comply with the specified requirements.

2.3. Data Protection Code of Practice

It is essential that those participating in mobile and remote working practices familiarise themselves with their responsibilities under the University’s Code of Practice on Data Protection. This can be found at [http://www.leeds.ac.uk/secretariat/data_protection_code_of_practice.html](http://www.leeds.ac.uk/secretariat/data_protection_code_of_practice.html).

* These Supporting Policies are in various stages of production and will be published at [http://www.leeds.ac.uk/informationsecurity](http://www.leeds.ac.uk/informationsecurity) as they are approved by the ISG.
In addition, the attention of those participating in remote working overseas is brought to Section 3.3.


3.1. The Desktop Anywhere Service

The University’s Desktop Anywhere Service is compatible with Microsoft, Macintosh and Linux systems and can be used wherever Internet connectivity is available.

This service provides the default means for mobile and remote working for users in the Admin domain. It must also be used by those in the DS domain who have a need to access classified information, as defined with the University’s Information Protection Policy, although other means of remote working, such as the University’s VPN service, Remote Desktop and FTP may be used by those in the DS domain to access less sensitive data that is not held on Corporate systems.

Alternatively, anyone in either the Admin or DS domain who simply needs to access their email is permitted to use the University’s Outlook Web Access facility, which is independent of the Desktop Anywhere Service but which incorporates the same security functionality. However, this service must not be used to carry and detach classified attachments as this information will then be stored on the machine from which the access is made.

Desktop Anywhere Service will be able to access the same resources that they access from their University desktop/laptop whilst on campus. The connection provided is secure, with data traffic encrypted, and the data is saved on the respective user’s ‘M’ drive instead of on the local hard drive of the machine being used for the access. As the connection between the remote computers and the University server is secure (https), no data is cached on the remote computers.

The Desktop Anywhere Service simply provides the means for users to access systems and data remotely in a secure and controlled way which minimises risk. It also prevents the currency of shared files being lost through the transfer of data between their storage facility and remote computers. When one user has accessed a shared document, anyone else trying to access it at the same time is informed that it is in use, and they will be granted read-only access to it.

Specific system policies (settings) have been applied to the Desktop Anywhere Service. These are automatically assigned to users of the service, and are based upon the group that each user is placed in, depending upon their user-profile. These policies, which have been agreed with the respective ‘data-owners’ have been defined to minimise risk. The controls prevent users from automatically caching data, and those with access to Corporate systems from saving such data to their local hard disk.

This prevents potentially sensitive University data from being accessed by unauthorised persons should a computer be sold on, stolen, or taken to a third party for repair, or as a result of non-University employees being permitted to use the computer in question. Under no circumstances

---

* Dial-up connectivity is not supported by ISS.
* Anyone who does not have a DS account may apply to ISS for one.
are these controls to be circumvented by transferring data via removable media, sending it as an email attachment or by any other means such as ftp.

The policies are as follows:

- Central Administration users are unable to save data locally from any application but may print locally.

- SAP and Banner users outside Central Administration are unable to save data locally from SAP or Banner, but are able to save data locally from other applications and may print locally.

- All other staff are able to save data locally and may print locally.

These policies apply whether the Desktop Anywhere Service is used remotely from off-campus or from the Wireless LAN, or from on-campus via a user’s work PC.

It is the responsibility of those leading project teams or research groups that are working on sensitive data, or under non-disclosure agreement, to ensure that appropriate controls are in place to protect that data. Where such work is being undertaken and mobile or remote access to respective data or systems is required, the ISS Helpdesk is to be contacted so that arrangements can be made for an appropriate policy to be implemented for the users requiring remote access.

3.2. The Creation and Storage of University Data on Privately-owned Computers

Privately-owned computers must not be used for the creation, storage or processing of:

- Classified data as defined in the Information Protection Policy; or,

- data which is categorised as being High or Medium Criticality data where there is no up to date backup or copy stored elsewhere.

3.3. Data Protection Implications - Remote Working Overseas

The Data Protection Act 1998 generally prohibits the international transfer of personal data (i.e. any data from which a living individual can be identified) into any country outside the European Economic Area (EEA), unless that country is designated as being ‘adequate’. At present, no country outside the EEA member states has been classed as adequate. (Annex A refers).

However, in certain circumstances, with specific controls in place, it is still possible for remote workers to process personal data whilst working overseas.

Any remote worker wishing to process personal data outside the EEA, without using the University’s Remote & Mobile Access Service, must contact the University’s IT Security Co-ordinator to establish the feasibility of doing so and to determine the specific conditions that will be applicable to them should this be feasible.

---

*SAP users are unable to print out locally as SAP does not support local printing.

**SAP users are unable to print out locally as SAP does not support local printing.

***This data must not be taken to or sent to any privately-owned computer by any means.
3.4. **Mobile Workers' Responsibilities**

Users are responsible for the safekeeping and protection of University-owned portable computers that have been issued or loaned to them.

Users in possession of University-owned portable computers are responsible for preventing unauthorised persons from using them and they must not loan them to others without prior authorisation.

Users of privately-owned computers that are or have been used to create, process, store or access University data are responsible for ensuring that non-members of the University do not gain access to that data when using their computers.

3.5. **Duty of Care**

Reasonable care and due diligence must be taken to prevent or reduce the possibility of loss or theft of University-owned portable computers.

Mobile workers are to take heed of the environment in which they are working and apply appropriate common-sense measures to protect University-owned portable computers and University data on both University-owned and privately-owned devices.

Losses of, or damage to, University-owned portable computers may be investigated in accordance with the *Security Incident & Computer Misuse Policy*. Where negligence on behalf of the custodian has resulted in the loss or damage action may be taken in accordance with University procedures.

Whilst there are many situations in which mobile workers will find themselves operating, there are four main categories to consider:

- working within the University’s premises;
- working outside the University’s premises;
- working in transit;
- transporting portable computers.

Control requirements associated with each of these are outlined below:

*Working within University Premises*

University-owned portable computers are not be left unattended on the University’s premises unless they are in a locked room or cupboard, with access restricted to local staff, or secured by an appropriate security device.

*Working outside University Premises*

When working outside The University’s premises, mobile workers are to be extra vigilant and apply appropriate precautions to protect portable computers in their care.

*Working in Transit*

Extra care must be taken when working in transit to prevent the disclosure or compromise of University information. Any unauthorised disclosure of personal information due to negligence on a user’s part could make that user liable to prosecution under the Data Protection Act 1998 (or
other legislation). This includes any case where details, which are governed by The Act, become public knowledge due to the theft of portable computers where it can be shown that the custodian was negligent in applying security controls. Sensitive University information must also be safeguarded against being viewed by unauthorised persons. Highly Confidential and Confidential data on University owned portable computers (protected by cryptographic controls in accordance with the Cryptographic Control Policy) must not be accessed or processed in public places where it could be overlooked by anyone who is not authorised to view it.

Transporting Portable Computers

Constant vigilance must be applied to reduce the possibility of loss or theft of University-owned portable computers, or the disclosure of University information on either University-owned or privately-owned equipment, whilst in transit. If University-owned portable computers, or privately-owned equipment that contains University data, have to be left in vehicles, they are to be placed in the boot or out of sight and the vehicle locked.

In a bid to reduce the chance of being ‘mugged’, those carrying laptop computers in public places may prefer to use bags other than those provided with the equipment, so that it is not obvious that they are carrying a valuable piece of equipment. However, in making this decision, the risk of damaging the laptop if it is accidentally dropped whilst not in its proper carrying case should be taken into account.

3.6. Network Connectivity

Portable computers which are connected to the University network must conform to the requirements which are specified within the Systems Security & Network Access & Management Policy. Connection of such devices is only to be undertaken in accordance with approved faculty/departmental controls and only with the correct level of authority.

Users of privately owned portable computers who wish to connect their devices to the University network are first required to register them with ISS in accordance with the Use of Computer Systems Policy, and are to ensure that their virus protection complies with University’s Virus Protection & Management Policy.

3.7. Data Backup

All mobile and remote users are personally responsible for ensuring that any University data on their machines (whether University-owned or privately-owned) is regularly and frequently backed up and that backup media is handled and stored in accordance with Data Storage & Backup Policy.

3.8. Security of Privately Owned Computers and the Protection of Data

Users, who access, produce or store University information on privately owned computer equipment, whether portable or static, are responsible for the security of them. In order to protect University information, such machines are to be protected by a firewall, operate anti-virus software (where necessary), and be kept up to date with security patches.

Guidelines for the security of PCs can be found at Annex B, for Linux users at Annex C and for Macintosh users at Annex D.
3.9. Incident Reporting

The loss of any University-owned portable information asset must be reported to the respective line manager, and where applicable, the IT Security Co-ordinator.

In cases of both loss and theft of University-owned portable computers, an evaluation of the sensitivity or criticality value of the lost information may be carried out in accordance with the Security Incident & Computer Misuse Policy to assess potential damage to the University's reputation and determine any counter-compromise actions.
4. **Annexes**


The 8th Principle of the Data Protection Act 1998 does not impose any restriction on the transfer of personal data to EEA countries. At the time of publication these are:

- Austria
- Belgium
- Bulgaria
- Cyprus
- Czech Republic
- Denmark
- Estonia
- Finland
- France
- Germany
- Greece
- Hungary
- Iceland
- Ireland
- Italy
- Latvia
- Liechtenstein
- Lithuania
- Luxembourg
- Malta
- Netherlands
- Norway
- Poland
- Portugal
- Slovakia
- Slovenia
- Spain
- Sweden

The following countries outside the EEA with their own data protection laws have been designated as ‘adequate’ by the European Commission:

- Argentina
- Canada
- Guernsey
- Isle of Man
- Switzerland
- United States of America (Safe Harbor list companies only).

For the latest up-to-date list of countries considered to be adequate, please see the European Commission’s data protection website at [http://www.europa.eu.int/comm/justice_home/fsj/privacy/thridcountries/index_en.htm](http://www.europa.eu.int/comm/justice_home/fsj/privacy/thridcountries/index_en.htm)
4.2. **Annex B – Security of Privately Owned Computers**

The use of privately-owned computers for University work imposes security responsibilities on the users.

Although many of the risks to University information or network resources are no different to those encountered by University-owned equipment, it is unlikely that the same processes and software are in place to protect privately-owned equipment. It is therefore important that steps are taken to protect privately-owned computers by:

- Maintaining up-to-date anti-virus software;
- Installing critical Windows security patches as soon as they become available;
- enacting a personal ‘firewall’ to protect your PC from being hacked, especially if you have a broadband connection; and,
- deleting data which has been cached by your computer.

**Anti-Virus Software**

The University has a site licence for McAfee’s VirusScan. This is one of the market leaders in the area of anti-virus software packages. The University's licence enables all members of staff to install it on their privately-owned computers with no additional cost.

It is strongly recommended that you install VirusScan on your PC. However, if you already own a different anti-virus software there is no reason why you should not continue to use the one you already have. The important point to remember is that whatever anti-virus package you use it MUST be kept up-to-date if it is to remain effective. New viruses are appearing all the time and most vendors of anti-virus software release several updates to their software each week. Anti-virus software which is out-of-date is worthless.

Fortunately you do not have to remember to update the software yourself as all these packages including VirusScan can be configured to periodically check for updates and download and install them without requiring that you do anything. It is recommended that you configure VirusScan to check for updates at least every day as it is not unknown for more than one update to be released within a single day.

If you want to know how you can obtain a copy of VirusScan please contact the ISS Help Desk.

**Automatic Updates**

New security vulnerabilities are being discovered in Windows software all the time and when they are Microsoft release updates to Windows XP and 2000 in the form of critical patches.

Fortunately you don’t have to download these patches and manually install them yourself. Both Windows 2000 and Windows XP incorporate a built-in feature called Automatic Updates.

When this is enabled your PC will periodically check with Microsoft’s servers to see if there are any new critical patches available. If there are it will download and install them for you. The extent to which you are aware that this is happening is configurable by you. For information on how to enable the automatic update feature select **Help and Support** from the **Start** menu. Then search the Windows help system for ‘Keeping Windows up-to-date automatically’. This will take you to step-by-step instructions on how to enable this feature.
Microsoft also provides an update service on their web site via http://windowsupdate.microsoft.com for the older versions of Windows operating system software. Versions of Windows prior to Windows 98 are not supported by service. Windows NT is supported but Microsoft do not guarantee that patches will be produced for newly discovered security problems within it.

**Internet Connection Firewall.**

Home PCs with network connections are deliberately targeted by people who wish to misuse them. Historically, home computers have lacked the network protection and automatic updating systems that are found on enterprise systems. One way of enhancing the protection of home computers is to utilise an Internet connection firewall.

A firewall is a piece of software or hardware, or a combination of both which runs on your PC and constantly listens for attempts by people on the network to make possibly illicit connections to your it. If you haven’t explicitly authorised this activity it will block such attempts. It’s particularly important if you have a broadband connection to the Internet that you operate a firewall.

Without a firewall and anti-virus software that checks for Trojans it will be easier for people to install software on your PC which will then give them remote control of it. Once they have control of your PC they potentially have access to the University’s information assets.

Windows XP has an in-built personal firewall which works fine, although more effective products can be bought. For information on how to enable the Windows XP Internet connection firewall select **Help and Support** from the **Start** menu. Then search the Windows help system for ‘Firewall’. This will take you to step-by-step instructions on how to enable this feature.

**Internet Cache**

As an employee you have an obligation to safeguard the security and confidentiality of the University’s sensitive information assets. Many people are unaware that when they view documents through the web, or as an email attachment, a copy of that document will be written to the hard disk of the PC being used, and they don’t have to explicitly save documents to the hard disk in order for copies to start accumulating there. Note, when using the University’s Remote & Mobile Access Service data is not cached.

When a PC is been used to access non-secure web sites it will have cached information stored on the local hard disk unless measures have been taken to remove this first. This may be available to others should it be taken to be repaired, or subsequently disposed of.

When you view a non-secure web page, your web browser, e.g. Internet Explorer, always writes a copy of that page to an area known as a cache. The next time you view it the browser can then read it from the cache rather than going back to the original website. This speeds up web surfing but in it also means that the information has been copied from its domain on to the PC’s hard disk.

Likewise if you view a word document or an Excel spreadsheet from a web page or one that has been sent to you as an email attachment, your PC will keep a copy locally even though you may never have been asked to save it.
You should configure Internet Explorer to delete the contents of your Temporary Internet Files folder each time you exit from the browser. You can do this by selecting – Tools – Internet Options – Advanced – Security and ticking the appropriate option.

Even though you have done this you should be aware that documents and a record of what you have been doing on the computer will build up in other areas on your local disk. There are free utilities you can download which will perform a more thorough clean up of you disk. One such tool you might wish to use is free and is called ‘Free Internet Eraser’. It can be downloaded from www.privacyeraser.com.

You are also encouraged to check your computer for spyware etc. periodically, by using proprietary software.
4.3. **Annex C – Linux Security Maintenance**

The use of privately-owned Linux machines for University work imposes security responsibilities on the users.

Although many of the risks to University information or network resources are no different to those encountered by University-owned equipment, it is unlikely that the same processes and software are in place to protect privately-owned equipment. It is therefore important that steps are taken to protect privately-owned computers by:

- Installing critical security patches as soon as they become available;
- enabling a personal ‘firewall’ to protect your PC from being hacked, especially if you have a broadband connection: and,
- deleting data which has been cached by your computer.

**Automatic Updates**

New security vulnerabilities are being discovered in Linux all the time and each distribution will release its own updates. These can be downloaded from the internet and installed. Fortunately most distributions have automatic update utilities. Redhat now only provides this service for Fedora users. It can be accessed via the up2date utility.


Security updates for the `stable` distribution of Debian Linux can be automatically installed by adding the following line to `/etc/apt/apt.conf` deb [http://security.debian.org/ stable/updates main contrib non-free and running apt-get update apt-get upgrade regularly.

Security fixes are included directly in the `unstable` distribution and - after a delay - in the `testing` distribution. Debian do not recommend using `testing` if you do not have other security measures in place.

Services started by the inetd or xinetd can be removed by modifying their entries in `/etc/inetd.conf`, `/etc/xinetd.conf` or `/etc/xinetd.d`.

Those that run independently are usually started by scripts in `/etc/init.d` or `/etc/rc.d/init.d`.

All distributions have a mechanism for removing or disabling these.

Linux systems have long used TCP-wrappers to limit access to services. If you wish to leave services running, it is recommended that you add the line -

```
ALL: ALL EXCEPT 127.0.0.1 to /etc/hosts.deny.  To disable all access by default and add explicit entries for services you wish to permit to in /etc/hosts.allow.
```

**Internet Connection Firewall.**

A firewall is a piece of software or hardware, or a combination of both which runs on your PC and constantly listens for attempts by people on the network to make possibly illicit connections to your it. If you haven’t explicitly authorised this activity it will block such attempts. It’s particularly important if you have a broadband connection to the Internet that you operate a firewall.
Most Linux installations incorporate a software firewall that should be installed when Linux itself is installed.

Home machines with network connections are deliberately targeted by people who wish to misuse them. Historically, home machines have lacked the network protection and automatic updating systems that are found on enterprise systems. One way of enhancing the protection of home machines is to utilise an Internet connection firewall. Without a firewall it will be easier for people to install software on your PC which will then give them remote control of it. Once they have control of your PC they potentially have access to the University’s information assets.

Hackers also take control of a machine to use that to hack into another machine. This would implicate you as it would appear as though the attack came from your machine.

Services that are not required should be turned off.

**Internet Cache**

As an employee you have an obligation to safeguard the security and confidentiality of the University’s sensitive information assets. Many people are unaware that when they view documents through the web, or as an email attachment, a copy of that document will be written to the hard disk of the machine being used, and they don’t have to explicitly save documents to the hard disk in order for copies to start accumulating there. Note, when using the University's Remote & Mobile Access Service data is not cached.

When a PC is been used to access non-secure web sites it will have cached information stored on the local hard disk unless measures have been taken to remove this first. This may be available to others should it be taken to be repaired, or subsequently disposed of.

When you view a non-secure web page, your web browser, e.g. Netscape, Firefox or Mozilla always writes a copy of that page to an area known as a cache. The next time you view it the browser can then read it from the cache rather than going back to the original website. This speeds up web surfing but in it also means that the information has been copied from its domain on to the machine’s hard disk. You should clear the contents of this cache regularly, but particularly if you have been accessing web sites that are restricted to University members or e-mail attachments concerning matters that should be kept within the University. Web browsers can be configured with a cache size of zero so no caching will ever occur.
4.4. **Annex D – Security Maintenance for Apple Macintoshes**

The use of privately-owned Apple Macintosh (Mac) machines for University work imposes security responsibilities on the users.

Although many of the risks to University information or network resources are no different to those encountered by University-owned equipment, it is unlikely that the same processes and software are in place to protect privately-owned equipment. It is therefore important that steps are taken to protect privately-owned computers by:

- Maintaining up-to-date anti-virus software;
- Installing critical security patches as soon as they become available;
- enabling a personal ‘firewall’ to protect your Mac from being hacked, especially if you have a broadband connection: and,
- deleting data which has been cached by your computer.

**Mac OS**

The most recent version of operating system for the Mac is known as “Mac OS X” (10.x) which is inherently more secure than previous versions (Mac OS 7.x – 9.x). The University would recommend that, wherever possible, machines are upgraded to the latest version of Mac OS X. The following steps apply to machines running Mac OS X.

**Anti-Virus Software**

The University has negotiated a limited number of licences for McAfee’s Virex product for Macintosh. This is one of the market leaders in the area of anti-virus software packages. The University’s licence enables members of staff to install it on their privately-owned computers with no additional cost but they must register their use of this product with ISS prior to use. In addition, any user who has taken out a .Mac subscription from Apple is also entitled to install and run a copy of Virex.

Although the number of viruses affecting the Mac are much fewer than their PC counterpart, it is strongly recommended that you install Virex on your Mac. However, if you already own a different anti-virus software there is no reason why you should not continue to use the one you already have. The important point to remember is that whatever anti-virus package you use it MUST be kept up-to-date if it is to remain effective. New viruses can appear at any time and most vendors of anti-virus software release several updates to their software each week. Anti-virus software which is out-of-date is worthless.

Fortunately you do not have to remember to update the software yourself as all these packages including Virex can be configured to periodically check for updates and download and install them without requiring that you do anything. It is recommended that you configure Virex to check for updates at least weekly.

If you want to know how you can obtain a copy of Virex please contact the ISS Help Desk.

---

1 Correct at time of writing. Please check with Apple for availability of this product.
**Automatic Updates**

New security vulnerabilities are being discovered in the Mac OS all the time and when they are Apple release updates to Mac OS X in the form of Security Updates.

Fortunately, you don’t have to download these updates and manually install them yourself. Mac OS X incorporates a built-in utility called Software Update. This is enabled by default and will automatically run weekly to check for new software and updates. For help on configuring Software Update, please type in “software update” into the Apple Help utility (choose Help from the menu bar). To run software update manually, select “Software Update” from the (blue) Apple in the menu bar.


Additional information for advanced Mac OS users

Mac OS X is configured by default to be a secure operating system. However, the system is based on an underlying UNIX operating system. If you enable additional functionality (such as enabling a file or web server for example) or enabling system-level (“root”) user accounts, then additional security measures will need to be taken. Please refer to the section for Linux security maintenance in this document for more information.

**Internet Connection Firewall.**

A firewall is a piece of software or hardware, or a combination of both which runs on your Mac and constantly listens for attempts by people on the network to make possibly illicit connections to your machine. If you haven’t explicitly authorised this activity it will block such attempts. It’s particularly important if you have a broadband connection to the Internet that you operate a firewall.

Mac OS X incorporates a software firewall that should be enabled.

The Firewall tab can be found in the “Sharing” system preference. Click on “Start” to enable the built-in Firewall.

Home machines with network connections are deliberately targeted by people who wish to misuse them. Historically, home machines have lacked the network protection and automatic updating systems that are found on enterprise systems. One way of enhancing the protection of home machines is to utilise an Internet connection firewall. Without a firewall it will be easier for people to install software on your Mac which will then give them remote control of it. Once they have control of your Mac they potentially have access to the University’s computers.

Hackers also take control of a machine to use that to hack into another machine. This would implicate you as it would appear as though the attack came from your machine.

As an extra precaution, you should not enable any of the services listed under the “Services” tab unless you know exactly what you are doing and the security implications of doing so.

**Internet Cache**

As an employee you have an obligation to safeguard the security and confidentiality of the University’s sensitive information assets. Many people are unaware that when they view
documents through the web, or as an email attachment, a copy of that document will be written to the hard disk of the machine being used, and they don’t have to explicitly save documents to the hard disk in order for copies to start accumulating there. Note, when using the University’s Remote & Mobile Access Service data is not cached.

When a PC is been used to access non-secure web sites it will have cached information stored on the local hard disk unless measures have been taken to remove this first. This may be available to others should it be taken to be repaired, or subsequently disposed of.

When you view a non-secure web page, your web browser, e.g. Safari, Internet Explorer, Netscape, Firefox or Camino, always writes a copy of that page to an area known as a cache. The next time you view it the browser can then read it from the cache rather than going back to the original website. This speeds up web surfing but in it also means that the information has been copied from its domain on to the machine’s hard disk. You should clear the contents of this cache regularly, but particularly if you have been accessing web sites that are restricted to University members or e-mail attachments concerning matters that should be kept within the University.

Using Apple’s Safari browser (the default in Mac OS X 10.2 or later) it is possible to empty the cache by selecting the “Empty Cache…” option from the Safari menu in the menu bar. In addition, under the Preferences menu, there is a “Security” tab which will allow you to block pop-up windows from opening. Pop-up windows are web pages that automatically open when you click on a link or visit a page. Sometimes, these windows can contain malicious content.

For more information on keeping your Mac secure, type in “security” into the Mac OS X Help utility (select Help from the menu bar) and then select the “Keeping your information safe” hyperlink.