Medical Sciences Division IT

Security Policy

Effective date: 1 September 2014

1 Overview

MSD IT provides IT support services support and advice to the University of Oxford Medical Sciences Division. Users of Information, Communications and Technology (ICT) within the University are subject in the first instance to the Information, Communications and Technology Committee (ICTC) regulations with subsequent amendments and available for review at:
http://www.admin.ox.ac.uk/statutes/regulations/196-052.shtml

MSD IT provide local services to sites operated by the Medical Sciences Division and the ICTC regulations alone do not fully provide for all the needs of a security policy covering these services. The current document provides additional policies and guidelines which apply to its services and users of its services within the Division. Effective security is a team effort involving the participation and support of every University employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these policies and guidelines, and to conduct their activities accordingly.

This Security Policy will be reviewed and updated on a yearly basis, or more frequently if necessary.

2 Definitions

To avoid ambiguities, particular terminology is used when explaining the policies:

- MUST: This word, or the terms "REQUIRED" or "SHALL", means that the item is an absolute requirement.
- MUST NOT: This phrase, or the phrase "SHALL NOT", means that the item is absolutely prohibited.
- SHOULD: This word, or the adjective "RECOMMENDED", means that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.
- SHOULD NOT: This phrase, or the phrase "NOT RECOMMENDED" means that there may exist valid reasons in particular circumstances when the particular behaviour is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behaviour described with this label

Abbreviations used in this document:

DHCP	Dynamic Host Configuration Protocol
ICT	Information, Communications & Technology
ICTC	Information, Communications & Technology Committee
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
IPSec	Internet Protocol Security (protocol suite for securing Internet Protocol (IP) communications)
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MAC address	Media Access Control address
MSD	Medical Sciences Division
MSD IT	Medical Sciences Division IT services
IT Services	Oxford University Information Technology Services (http://www.it.ox.ac.uk)
OxCERT	Oxford University Computer Emergency Response Team (http://help.it.ox.ac.uk/network/security/index)
OWL	Oxford Wireless LAN (http://help.it.ox.ac.uk/network/wireless/services/owl/index)
PDA	Personal Digital Assistant
SNMP	Simple Network Management Protocol

SNMPv2	Simple Network Management Protocol version 2
SSH	Secure Shell
SSID	Service Set Identifier
SSL	Secure Sockets Layer
VPN	Virtual private network

3 Acceptable Use Policy

In supporting an Acceptable Use Policy, it is not the intention of MSD IT to impose additional restrictions that are contrary to the University of Oxford's established culture of openness, trust and integrity. Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, internet browsing, and file transfer, are the property of the University of Oxford. These systems are to be used for business purposes in serving the interests of the University in the course of normal operations.

3.1 Purpose

The acceptable use policy defines what behaviour is acceptable with regard to the use of ICT facilities operated by MSD IT on behalf of the University.

3.2 Policy

Acceptable use is defined in the University's ICT regulations to be found at:
http://www.ict.ox.ac.uk/oxford/rules/

4 Password Policy

4.1 Overview

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of MSD IT-administered networked systems. As such, all users of our systems (including contractors and vendors with access to MSD IT systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

4.2 Purpose

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords and the frequency of change.

4.3 Scope

The scope of this policy includes all who have or are responsible for an account (or any form of access that supports or requires a password) on any system installed at any MSD IT-administered facility, or that has access to an MSD IT-administered network.

4.4 Policy

a. All user-level passwords (e.g., web, desktop computer, etc.) must be changed at least every 12 months.

b. All system-level passwords (e.g., root, enable, admin, application administration accounts, etc.) must be changed at least every 12 months. All production system-level passwords must be entered in the MSD IT-administered global password management database.

c. All user-level and system-level passwords must conform to the following characteristics:

i.	Minimum password length:	8 characters
ii.	Minimum number of lowercase characters:	1
iii.	Minimum number of uppercase characters:	1
iv.	Minimum number of numeric characters:	1
v.	Maximum sequential repetition of a character:	2
vi.	Minimum number of different characters:	5

d. Users must not share University passwords with ANYONE, including IT support staff, administrative assistants or secretaries, line manager, family members, etc.

e. Passwords must not be inserted into email messages or other forms of electronic communication.

f. Users must not write down passwords or password hints (e.g., "my family name")

g. Users must not reveal a password on questionnaires or security forms.

h. If an account or password is suspected to have been compromised, users must report the incident to MSD IT.

i. Where SNMP is used, the community strings must be defined as something other than the standard defaults of "public," "private" and "system" and must be different from the passwords used to log in interactively. A keyed hash must be used where available (e.g., SNMPv2).

j. Application developers must ensure their programs contain the following security precautions.
   i. Applications must not store passwords in clear text or in any easily reversible form.
   ii. Applications must provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.
   iii. Applications must support LDAP over SSL to compare a given password with the Universal password stored in MSD IT eDirectory, wherever possible.

4.5 Issuing of passwords

Users must register with MSD IT by filling in a form available on the MSD IT web site (http://www.imsu.ox.ac.uk/Registration). The user must call in person to their local MSD IT office to obtain their username and password. The user must show proof of their identity by presenting a valid University card, and sign a copy of their application form to show that they understand their responsibilities with respect to data protection and terms of use, etc. For users who are not local to MSD IT offices (e.g. working abroad), the credentials shall be sent out in a sealed envelope to the user's Departmental Administrator (or equivalent) whose responsibility it is to convey that envelope to the end user.

If a password needs to be recreated by MSD IT, the user must call in person to the MSD IT offices so that their identity can be verified. For users who are not local to MSD IT offices, the new password shall be sent out in a sealed envelope.

Under no circumstances will a password be conveyed to the user over the phone.

4.6 Guidelines

Please see Appendix 1 for some guidelines on how to create strong passwords, and protect them.

4.7 Other passwords used in the Oxford University environment.

It is important to differentiate between the password needed to access the MSD IT services (network access, files storage), and those needed to access 1) a Nexus email account, and WebLearn (called the Oxford or SSO password), and 2) the VPN service. The latter two services have their own password policies and are administered by the Oxford University IT Services (http://help.it.ox.ac.uk/registration/index#passwords).

5 Access Policy

The purpose of this policy is to define standards for connecting to MSD IT-administered networks from any host. These standards are designed to minimize the potential exposure of the University to damages which may result from unauthorized use of MSD IT-administered resources. Damages include the loss of sensitive or confidential data, intellectual property, damage to public image, damage to critical MSD IT internal systems, etc.

5.1 Scope

This policy applies to all employees, contractors, vendors and agents with a University-owned or personally-owned computer or workstation used to connect to an MSD IT-administered network or service. MSD IT operates and manages data networks and networked services for the Medical Sciences Division Departments on various sites in Oxford. This policy applies to on-site connections made from all networks administered by MSD IT and to remote connections made from outside the MSD IT networks which include, but are not limited to, VPN and SSH.

5.2 Policy

Only users with a valid University card shall be allowed to access the MSD IT networks. Departmental administrators are responsible for arranging applications for their staff to the University Card Office (http://www.admin.ox.ac.uk/card/apply/). This includes any temporary staff that might be hired for short periods.

All users shall have individual login access to the MSD IT networks. There will be no open access logins (i.e. guest, temp or public logins). The exceptions to this are where a generic username needs to be used to allow an item of lab equipment to run or a lecture room presentation computer to be used by a non-cardholder. In this case the generic logon is restricted to the specific item of equipment itself and cannot be used to access any network drives or to logon to the network itself through a different client machine.

The management and control of user access rights will be the joint responsibility of the MSD IT, local IT coordinators and individual Departmental or Unit managers. Authorisation of individual user access rights is the responsibility of Departmental administrators or Unit managers. Every user, as a minimum, is provided with access to a server based 'home' drive, which provides networked storage space for their personal use. In addition, each user will be allocated access rights to additional 'standard' shared network resources which are granted based on their Department or Unit affiliation. If additional group or Unit drives need to be accessed by a user, the owner of the data must authorize the granting of user access rights by filling in a form available on our web site (http://www.imsu.ox.ac.uk/Registration).

The management and control of computer desktops and laptops will be the joint responsibility of the users, MSD IT, local IT coordinators and individual Departmental or Unit managers. All computers must be registered in the MSD IT database before they are able to obtain an IP address with which to connect to the MSD IT networks.

It is the responsibility of employees, contractors, vendors and agents accessing the MSD IT network services to ensure that their computer is running fully patched operating systems, and is running active and current 'anti-virus' software as per current recommendations by MSD IT. Only machines with operating systems that are within their support lifecycle will be supported by MSD IT; machines with operating systems outside of the manufacturers support will not be allowed on the network.

It is the responsibility of employees, contractors, vendors and agents accessing the MSD IT network services to ensure that their remote access connection is given the same consideration as their on-site connection to those services. Please review the University of Oxford's ICTC regulations for specific rules relating to remote access (http://www.ict.ox.ac.uk/oxford/rules/).

5.3 Leavers

When the University card of a user expires, their access rights to the MSD IT networks will be automatically revoked. Access rights will be reactivated upon the presentation of a new valid University card. Exceptionally, if authorized by their Departmental administrator less than twelve months after the expiry of their credentials, a user will be allowed to access their network 'home' drive for one 7-day period.

Twelve months after the expiry of their credentials, user data on all MSD IT file servers will be deleted. The data stored on the MSD IT backup systems will also be deleted.

6 Mobile Device (laptops and tablets) Policy

The purpose of this policy is to establish an authorised method for controlling mobile computing and storage devices that contain or access information resources on MSD IT-administered networks.

6.1 Scope

This policy applies to all employees, contractors, vendors and agents with a University-owned or personally-owned laptop computer or other mobile computing device used to connect to an MSD IT-administered network or service. Only users with a valid University card shall be allowed to access the MSD IT networks as stated in section 5.2 above.

6.2 Policy

Mobile computing and storage devices accessing an MSD IT-administered network or service must be approved prior to connecting to the network. MSD IT will register the device for use on its networks after ensuring that it is secure and manageable, and that sufficient information has been provided to trace the device and /or its owner. MSD IT may need to install additional software on the device to enhance their ability to remotely manage and/or monitor the device

Where a user is not able to provide the information above or allow the device to be adapted for use on MSD IT-administered networks, the user may be offered access to the University of Oxford OWL or eduroam network where this is available:
http://help.it.ox.ac.uk/network/wireless/services/owl/visitor/index.

Please review the University of Oxford's ICTC regulations for specific rules relating to the connection of computing devices to the University network
(http://www.admin.ox.ac.uk/statutes/regulations/196-052.shtml).

7 Electronic Mail Usage Policy

7.1 Scope

MSD IT does not manage a user-based email system. The email service is provided centrally by IT Services for the whole of the University of Oxford (http://help.it.ox.ac.uk/nexus/index). Please refer to the IT Services information security policy for more details:
http://www.it.ox.ac.uk/policies-and-guidelines/information-security-policy

MSD IT runs a mailing list system that is made available to Departments and Units. The scope of this policy includes all who are responsible for a mailing list on the system administered by MSD IT.

7.2 Policy

MSD IT is responsible for the initial creation of mailing lists, the maintenance and backup of the service, and the scanning of messages with anti-virus software. List owners will be responsible for managing the subscriptions and general configuration of the mailing lists. Mailing list traffic should be restricted to work-related information. This therefore excludes the use of the mailing list system for advertising personal items for sale, for example.

8 Anti-Virus Policy

8.1 Scope

This policy applies to all employees, contractors, vendors and agents with a University-owned or personally-owned server, desktop or laptop computer or other mobile computing device connected to an MSD IT-administered network.

8.2 Policy

Anti-virus software provided by MSD IT via a site-license must be used on all systems connected to an MSD IT-administered network. The preferred method of software installation is via the automated service provided by MSD IT. All file servers must have an anti-virus application installed that offers protection to files and applications running on the target system.

All installed anti-virus software must be configured to update automatically.

All end-user systems should have an anti-spyware application installed that offers real-time protection to the target system.

8.3 Guidelines

Please see Appendix 2 for some guidelines on how to protect computers against viruses.

9 Server Security Policy

The purpose of this policy is to establish standards for the base configuration of internal server equipment that is owned and/or operated by MSD IT. Effective implementation of this policy will minimize unauthorized access to the University's proprietary information and technology.

9.1 Scope

This policy specifically applies to server equipment owned and/or operated by MSD IT, and to servers registered under any MSD IT-administered network. Desktop machines and laboratory/test equipment are not relevant to the scope of this policy.

9.2 Policy

All internal servers deployed by MSD IT must be owned by an operational group that is responsible for system administration. Approved server configuration guides must be established and maintained by each operational group. Operational groups should monitor configuration compliance and implement an exception policy tailored to their environment. Each operational group must establish a process for changing the configuration guides, which includes peer review and approval.

Servers must be physically located in an access-controlled environment.

Servers must be registered in the MSD IT network management system. As a minimum, the following information is required to positively identify the point of contact:

- Server contact(s) and location, and a backup contact
- Hardware and Operating System/Version
- Main functions and applications, if applicable

Information in the MSD IT management system must be kept up-to-date.

Configuration changes for production servers must follow the appropriate change management procedures.

Services and applications that will not be used must be disabled where practical.

The most recent security patches must be installed on the system as soon as practical, the only exception being when immediate application would interfere with business requirements.

If a method for secure channel connection is available, privileged access must be performed over secure channels, (e.g. encrypted network connections using SSH or IPSec).

Security-related events must be reported to OxCERT, who will review logs and report incidents to IT management. Corrective measures will be prescribed as needed. Security-related events include, but are not limited to:

- Evidence of unauthorized access to privileged accounts
- Anomalous occurrences that are not related to specific applications on the host.

9.3 Guidelines

Please see Appendix 3 for some guidelines on how to configure servers.

10 Wireless Infrastructure Policy

This policy specifies the conditions that wireless infrastructure devices must satisfy to connect to MSD IT-administered networks. Only those wireless infrastructure devices that meet the standards specified in this policy or are granted an exception by the MSD IT are approved for connection to a MSD IT-administered network.

10.1 Scope

This policy applies to all wireless infrastructure devices that connect to a network administered by MSD IT and that provide wireless connectivity to endpoint devices including, but not limited to, desktops, laptops, tablets, eReader, cellular phones, and personal digital assistants (PDAs). This includes any form of wireless communication device capable of transmitting packet data.

10.2 Policy

All wireless infrastructure devices that connect to an MSD IT-administered network must:

- Abide by the following standards specified in the Mobile Wireless Networking Regulations as approved by the ICTC:
  http://www.it.ox.ac.uk/network/wireless/rules/
- Maintain a hardware address (MAC address) that can be registered and tracked.
- Be installed, supported, and maintained by MSD IT.
- Not interfere with wireless access deployments maintained by other organisations
- Only authorized wireless networks are allowed
- The SSID OWL, or any prefix or suffix on that identifier may only be used according to a naming scheme released by IT SERVICES, and the OWL family of SSIDs must be used only to provide standardized OWL services
- The SSID eduroam, or any prefix or suffix on that identifier, may not be used except for the purposes of the international eduroam service
- All wireless networks must be registered with IT Services by the local IT support staff
- The wireless network must be separated from any other University connected network
- User authorization is required before network access is allowed
- Strong data encryption must be used
- Hosts offering services that compromise security must not be permitted (examples of this include proxy, relay, DHCP, routing services etc.). This refers to client operations, not system provided facilities.
- All associations must be recorded.

10.3 Recommendations

Please see Appendix 4 for a summary of IT Services recommendation.

11 Enforcement

MSD IT supports and assists in the enforcement of all the regulations listed above across the University of Oxford Medical Sciences Division.

Any employee found to have violated University ICTC regulations may be subject to disciplinary action.

MSD IT may remove access rights to its systems and administered networks from users who contravene any of the above policies.

Appendix 1 Password Creation Guidelines

Passwords are used for various purposes at the University. Some of the more common uses include: user-level accounts, web accounts, email accounts and screen saver protection. The best practice suggestions for password creation and protection are summarized below.

Strong passwords have the following characteristics:

- They contains a mixture of both upper and lower case characters (i.e., a-z, A-Z)
- They have digits and punctuation characters as well as letters: i.e., 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)
- They are at least fifteen alphanumeric characters long.
- They are not a word in any language, slang, dialect, jargon, etc.
- They are not based on personal information, names of family, names of pets, phone numbers, car registration number, etc.
- They are never written down or stored on-line. Try to create passwords that can be easily remembered.
- One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.
  Please do not use these examples !

Password Protection Standards

- Do not use the same password for University accounts as for other non-University access (e.g. personal ISP account, banking services, benefits, etc.). Where possible, don't use the same password for various University access needs. For example, select one password for the Nexus email system and a separate password for MSD IT systems.
- Don't reveal a password to ANYONE in person or over the phone
- Don't reveal a password in an email message
- Don't reveal a password to a manager, or a colleague before going on holiday
- Don't talk about a password in front of others
- Don't hint at the format of a password (e.g., "my family name")
- Don't reveal a password on questionnaires or security forms.
- Don't share a password with family members

- If someone demands your password, refer them to this document or have them call the MSD IT Help desk

- Do not use the "Remember Password" feature of applications (e.g., Eudora, Outlook, Thunderbird, Mac Mail, etc.).

- Do not write passwords down and do not store them anywhere in your office. Do not store passwords in a file on ANY computer system (including smart phones, tablets, or similar devices) without encryption.

- Although the MSD IT Policy enforces a password change every 12 month, it can be good to change passwords more frequently.

- If an account or password is suspected to have been compromised, report the incident to MSD IT and change all passwords.

Appendix 2 Anti-Virus Protection Guidelines

- Always run the standard, supported anti-virus software which is available from MSD IT.
- Anti-virus software installed by MSD IT must be configured to update automatically. On personally-owned or remote systems, the user should ensure that updates are performed frequently.
- NEVER open any files or macros attached to an email from an unknown, suspicious or untrustworthy source. Treat with caution files or macros attached to emails that you were not expecting to receive. It is suggested that you contact the sender to verify the origin of the attachment or delete these attachments immediately, then empty your Trash or Wastebasket.
- Delete spam, chain, and other junk email without forwarding.
- Never download files from unknown or suspicious sources.
- Always scan a USB memory stick, floppy diskette or other removable media from an unknown source for viruses before using it.
- Back-up critical data and system configurations on a regular basis and store the data in a safe place.

Appendix 3 General Server Configuration Guidelines

- Access to services should be logged and/or protected through access-control methods such as TCP Wrappers, if possible.

- Trust relationships between systems are a security risk, and their use should be avoided. Do not use a trust relationship when some other method of communication will do.

- Always use standard security principles of least required access to perform a function. Do not use privileged accounts when a non-privileged account will do.

- All security related logs should be kept for a minimum of 6 months.

Appendix 4 Summary of IT Services Recommendations Regarding the Wireless Infrastructure

(for more details http://help.it.ox.ac.uk/network/wireless/rules/index#recommendations)

- The IEEE 802.11b wireless standard should be supported. This is the Wi-Fi standard and the one that will most commonly be available on clients
- Only Wi-Fi approved equipment should be used
- Compatibility between equipment cannot be guaranteed unless it has been tested. IT Services Wi-Fi approved equipment has been through the approval process
- Only the IP protocol should be supported
- IP is the protocol of choice - all others are treated as legacy protocols by the University and have dwindling support
- The minimum necessary power to provide coverage of your area should be used
- Use of high signal strengths causes the signal to propagate into areas where coverage may not be required and, indeed, could provide potential connectivity to people for whom it is not intended
- Reducing power levels reduces leakage and interference problems
- Use different frequencies to those of nearby access points (which may be in another building)
- Suitable choices of channel allocations can reduce interference between multiple access points, thus improving signal strength to clients and allowing higher throughput. The limited number of available channels (three) at 2.4 GHz means that this is recommended
- High bandwidth utilization applications should not be allowed
- As wireless technology is a shared medium with limited bandwidth, it is possible for one user to utilize the majority of the bandwidth. If anyone has high bandwidth needs then a normal 'wired' connection should be used