Medical Sciences Division IT Services (MSD IT)

Security Policy

Effective date: 1 December 2017

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 provides local services to departments 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 Information 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 be familiar with these policies and guidelines, and to conduct their activities accordingly.

This Security Policy will be reviewed annually, 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 not optional.
- 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 be valid reasons in particular circumstances not to implement a particular item, but the full implications must be understood and carefully weighed before doing so.
- SHOULD NOT: This phrase, or the phrase "NOT RECOMMENDED" means that there may be 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 action 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 IT Services (http://www.it.ox.ac.uk)
OWL	Oxford Wireless LAN (http://help.it.ox.ac.uk/network/wireless/services/owl/index)
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
WDE	Whole Disk Encryption

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, printers, tablets, mobile phones, 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 described in the University's ICT regulations to be found at:
http://www.it.ox.ac.uk/rules

4 Password Policy

4.1 Overview

Passwords are an important aspect of ICT and 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 of suitable length and complexity.

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 be at least 16 characters long and should include several different classes of character, with spaces being acceptable.

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, particularly on those reached by following a link in an email that purports to be from an IT provider.

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., SNMPv3).

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, where possible, 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 the 'New user' form available on the MSD IT web site (http://www.imsu.ox.ac.uk/Registration). On allocation of an individual's username and password, MSD ITS will send the requester an email message (to their University of Oxford email address) containing instructions so they can activate their account by visiting the MSD IT web site offering the online activation interface. On completion of the activation process, the user receives their username by email to their University of Oxford email address.

During the activation process, the user will be required to create their own security and answer question that could be used later for self-service recovery, should the user forget their password. The self-service password recovery service is available from the MSD IT account manager web site (https://userdb.imsu.ox.ac.uk/).

When a user cannot remember the answer to their security question, MSD IT will reset the user's password and instruct the user to use the online activation interface. An activation code is automatically generated and sent to the user's University of Oxford email address. This code needs to be used by the user to complete the password reset process.

If the user doesn't have a University email address, MSD IT will require the approval of the user's Departmental Administration before allowing the use of a non-University email address in the activation process. Alternatively the user will be invited to the MSD IT office to create their password themselves on presentation of appropriate photographic identification.

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

4.6 Guidelines

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, MSD VPN), and those needed to access 1) a Nexus email account, and WebLearn (called the Oxford or SSO password), and 2) Remote Access (eduroam / OWL / VPN). The latter two services have their own password policies and are administered by Oxford University IT Services (https://register.it.ox.ac.uk/self/index).

5 Access Policy

The purpose of this policy is to define standards for connecting to MSD IT-administered networks from any computer or device. 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 and services. 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 the 'User access rights' form available on our web site (http://www.imsu.ox.ac.uk/Registration).

The management and control of desktop computers, mobile devices, and laptops will be the joint responsibility of the users, MSD IT, local IT coordinators and individual Departmental or Unit managers. All devices 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.

Devices that have not been active on an MSD IT managed network for a period of 6 months may have their network access suspended by MSD IT.

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.it.ox.ac.uk/rules).

5.3 Leavers

When a person's University card 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 to MSD IT. 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, tablets and smartphones) 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 in the event of loss. MSD IT may need to install additional software on the device to enhance their ability to remotely manage and/or monitor the device and will insist on Whole Disk Encryption (WDE) for laptops that are likely to hold personal or sensitive personal data as defined by the Data Protection Act 1998. Use of the central University WDE service is recommended as it provides auditability, recoverability and strong encryption but if that is not appropriate then a suitable alternative such as bit locker, file vault or Veracrypt is acceptable.

Users must ensure that data on their mobile device is appropriately protected from unauthorised access by setting a strong password/PIN-protected lock-screen to come on automatically when the device is not in use. The use of a longer PIN or password is strongly recommended. We do not recommend unlock "patterns" but will accept the user of fingerprint unlocking so long as only the fingerprints of the device owner are registered on it. Devices should also be encrypted and configured to require a passcode at restart.

When a device cannot be adapted/configured for use on MSD IT-administered networks, the user may use the University of Oxford OWL or eduroam wireless 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 an email system. Oxford University's 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

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.

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

Anti-spyware software is also recommended for all computers.

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 physical or virtual 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 in 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 a secure, 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 the University Information Security team (https://www.infosec.ox.ac.uk), 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.

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, eReaders, smart phones, and printers. 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://help.it.ox.ac.uk/network/wireless/rules/index
- 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 and then to its strict standards.
- 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
- Devices offering services that could compromise security or network use by other devices must not be permitted (examples of this include proxy, relay, DHCP, routing services etc.). This refers to client operations, not system provided facilities.

11 Enforcement

MSD IT supports and assists the appropriate authorities 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 by the appropriate authorities.

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