Medical Sciences Division IT

Summary of User Security Policy

MSD IT operates and manages data networks and networked services for the Medical Sciences Division Departments on various sites in Oxford. This user policy applies to everyone using networks administered by MSD IT and to remote connections made from outside the MSD IT networks.

Access Policy

This policy applies to all users with a University-owned or personally-owned computer connected to a network or service administered by MSD IT.

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 need to register with MSD IT to obtain a username and password in order to login to the MSD IT networks. The registration process requires users to fill in a form available on our web site (http://www.imsu.ox.ac.uk/Registration). 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).

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.

All computers to be used to connect to the MSD IT networks must be registered in the MSD IT database before they are able to obtain an IP address that will allow the connection to the MSD IT networks. It is the responsibility of all users 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.

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, users' data on all MSD IT file servers will be deleted. The data stored on the MSD IT backup systems will also be deleted.

Password Policy

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

b. All user-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

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

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

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

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

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

h. For some advice, please see the document "Guidelines on how to create strong passwords and protect them" available on MSD IT web site:
http://www.imsu.ox.ac.uk/sites/default/files/content/files/MSD IT Password Guidelines.pdf

Issuing of passwords

Users must register with MSD IT by filling 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 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 transmitted to the user over the phone.

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 Computing Services (OUCS) (http://help.it.ox.ac.uk/registration/index#passwords).