MSD IT High Compliance system

Fact sheet

The MSD IT High Compliance system is a service for Clinical Trials Units (CTUs) and Medical Division Departments or Units who need to securely access critical applications, and manipulate and store very sensitive data.

Using a Remote Desktop Connection, users gain access to a virtual desktop that runs on a server. Only the video display is transmitted on the network. The data stays on the server, and the applications and programs run on the server.

As such the new system is not intended as a repository or archive of sensitive data. The primary purpose is to allow people to manipulate sensitive data as required by regulatory bodies.

This document highlights a few features that have been implemented to make this system as secure as possible, while maintaining some flexibility for the users to carry out their work involving sensitive data. The top priority is SECURITY.

Data accessible to this system need to be imported by a user nominated by the group leader of the relevant research team. The group leader will be considered the "data owner" and will be responsible for discussing the various security aspects with MSD IT, the granting of rights and permissions, and confirming which users need to access the data.

1. Password change

In order to access the Password Change wizard:

When connected to the Remote Desktop system:

1. Click on the Start button (bottom left of the window) --> Windows Security --> Change a password

2. Click on the button representing your username, then put your old password, your new password (twice), and click on the arrow pointing to the right. In the next window, you can click on the "Password Policy" button to review the password policy, or on the "OK" button to confirm the change you have made.

2. Internet access is disabled

Access to the Internet is disabled on this system to prevent sensitive data from leaking (intentionally and unintentionally). Email clients are also not available for the same reason. If requested by the group leader, very restricted Internet access can be granted (e.g. access to a database on a departmental web site).

3. No access to local drives

The local hard disks, USB sticks, CD/DVD drives and all your normal network drives are not available to the Remote Desktop Connection to prevent sensitive data from leaking (intentionally and unintentionally).

4. No access to server C drive

There is no need for any user to access the server C drive. Users have access to a personal H drive, and if arranged with the group leader, one or more Departmental shared network drives can be made available.

5. Network drives

Users have access to a personal H drive for their use. This H drive is only accessible from within a Remote desktop session and is different from the H drive users might have on the standard MSD IT (Novell) system.

Depending on requirements, users might also have access to one or more drives that may or may not be shared with other users in the same research group.

6. Personal folders redirection

No files can be saved on the C drive of the server offering the Remote Desktop Connection sessions.

The "My Documents", the content of the "Start" menu and the "Desktop" are redirected to folders on the user's H drive.

Additionally, a folder named "Application Data" is also saved on the user's H drive. This contains applications settings that are specific to the user. In summary, four folders are created automatically on the H drive of each user, and these folders should not be deleted.

N.B. In some cases, Folder redirection will only work after the 2nd login.

7. File transfer in and out of the system

Files can be transferred into the system or out of the system via a special interface available using the File Transfer application from within a Remote Desktop Connection session. For this purpose you have a network drive named the T drive inside the High Compliance are, and another T drive inside the standard MSD IT/Novell system. It is important to remember that the T drive inside the standard MSD IT/Novell system is not as secure as the T drive inside the High Compliance system. Files should be kept there for the shortest possible period of time. Note that for the transfer system to work properly, files on the T drive need to be inside the folder named with your username.

Transfer in

1. In the standard MSD IT/Novell file system put your files inside the folder with your username in your T drive.
2. In the Remote Desktop session open the File Transfer application (icon with white arrow on green background) and go to:
   http://tonus.imsu.ox.ac.uk/hctfer/ (this is only available from inside a Remote Desktop session)
3. select "High Compliance File Transfer" on the left hand side
4. click on the "Transfer in" button
5. you will be presented with the list of files that are ready to be transferred. Below that list you should fill the box asking you for the reason for the transfer. The manager of the project will receive a notification of all the transfers. When ready, click on "Confirm Transfer".
6. when the transfer is completed, you will be shown the list of transferred files, confirming the transfer
7. finally it will be important to move the files from the T drive in the Remote Desktop session into your H drive or any other shared drive. Files left on the T drive will be deleted after 24 hours.

Transfer out

1. In the High Compliance Remote Desktop session put your files inside the folder named with your username in your T drive.
2. In the Remote Desktop session open the File Transfer application (icon with white arrow on green background) and go to:
   http://tonus.imsu.ox.ac.uk/hctfer/ (this is only available from inside a Remote Desktop session)
3. select "High Compliance File Transfer" on the left hand side
4. click on the "Transfer out" button
5. you will be presented with the list of files that are ready to be transferred. Below that list you should fill the box asking you for the reason for the transfer. The manager of the project will receive a notification of all the transfers. When ready, click on "Confirm Transfer".
6. finally, when the transfer is completed, you will be shown the list of transferred files, confirming the transfer
7. finally it will be important to move the files from the T drive in the Remote Desktop session into your H drive or any other shared drive.

   Files left on the T drive will be deleted after 24 hours.

8. Desktop colour and arrangement

Users can customize their work space on the Remote Desktop Connection. They can select the colour of the desktop background, modify the resolution, create shortcuts at will, etc.

To modify the appearance of the desktop, users will first need to start the Remote Desktop Connection session from the Start menu:

1. Start menu --> All Programs --> Accessories --> "Remote Desktop Connection". When the window opens, click on the "Options" button (bottom left), select the tab named "Experience" and enable "Desktop background" by putting a check mark in front of it. To change the desktop resolution, select the "Display" tab, and configure the "Display Configuration"

2. Then click on the "Connect" button, and login as usual. Finally, within the Remote Desktop Connection session, click on the Start button --> "Control Panel", select "Display", then "Change desktop background".

9. Maintenance of the system

In order to maintain the system with the most up-to-date applications and security patches, the servers might be rebooted during a 2 hour windows: between 3:00am and 5:00 am without warning any day of the week.

10. Log off

To terminate a Remote Desktop Connection session, users will need to initiate the log off sequence by clicking on the Start button and selecting "Log off".

This closes all applications and files. The system will ask whether the user wants to save any unsaved data. This is the safest way to leave the session and not lose any data.

11. Lock this computer

To temporarily suspend a Remote Desktop Connection session, users can "lock" the session. Typically this allows the user to leave their desk with files opened in the Remote Desktop session and make sure no-one can see their data. The user's password will be required to allow the unlocking of the session. Applications and open files will remain opened.

Note that after 6 hours in this state, your session will be terminated, and all programs will be closed which will result in loss of data for any file that had not been saved before the locking of the session. It is advisable to save all open files before activating this feature.

This feature is available from the Start button (bottom left of the window):

- Windows Security --> Lock this computer.
- Alternatively, this can be activated by simply closing the Remote Desktop Connection window (clicking on the top corner "X").

12. Auto-save

It is good practice to setup auto-save in all applications if available. It is certainly available in Microsoft Office applications such as Excel. Auto-save can automatically save open files at a specified time interval. As your Remote Desktop Connection session runs alongside your other applications on your computer, it is recommended that you take this additional precaution to make your data safe.

13. Maximum session duration

All Remote Desktop Connections sessions are limited to 8 hours. When the time limit is reached, the session will be automatically closed after presenting a 2-minute warning to the user. All the applications and files will then be closed automatically. If open files have not been saved by the user, data may be lost.

It is advisable to close sessions before the 8-hour limit. It is considered good practice to close sessions when one has to leave one's computer for more than a few minutes, e.g. when going for lunch.

14. Maximum idle time

Idle Remote Desktop Connections sessions are limited to 6 hours. When the time limit is reached, the session will be automatic closed after presenting a 2-minute warning to the user. All the applications and files will then be closed automatically. If open files have not been saved by the user, data may be lost.

It is advisable to close sessions if they are going to be idle for some time. It is considered good practice to close sessions when one has to leave one's computer for more than a few minutes, e.g. when going for lunch.

15. Maximum time disconnected

Closed Remote Desktop Connections sessions are limited to 3 hours. That includes sessions that are locked by the users. When the time limit is reached, a closed session will be automatically deleted from the server.

(continued on next page)

All the applications and files will then be closed automatically. If open files have not been saved by the user, data may be lost.

It is advisable to close sessions if they are going to be idle for some time. It is considered good practice to close sessions when one has to leave one's computer for more than a few minutes, e.g. when going for lunch.

16. Auto screen saver

When a Remote Desktop Connection session is idle for 5 minutes, the screen saver will be initiated. The session window will stay open, and the user will need to enter their password to continue the session (the programs keep running). If the session is not resumed within 6 hours, the maximum idle time limit process will terminate the session as indicated above (paragraph 11), with possible data loss.

17. Sophos anti-virus is installed

The server providing Remote Desktop Connections is scanned regularly for viruses. The anti-virus software is also configured to check files at access time (e.g. when opened, copied, moved, etc.). If a user wants to specifically scan their H drive or one of the shared network drives, Sophos is available for manual scan:

- Go to the Start menu, select All Programs, select Sophos, then select "Sophos Endpoint Security and Control".
- Click on Scan (_not_ on "Scan my computer"), and select "Setup a scan". Select the drive you want to scan and click on "Save and start".

18. Printing

Printing is only allowed on specially registered network printers.

Printing is not allowed on local printers, or network printers used on the standard MSD IT network.

If users need to print data from their Remote Desktop Connection sessions, the group leader will need to nominate one or more network printers for use by the team. The group leader will need to be satisfied with the location of the network printer and its security.

Printers can be existing ones that are already on the standard MSD IT network, but they will need to be registered again for use with this new system. A local IT support officer might be required to arrange for the printer to be connected to the system.

When printing for the first time, users will be asked to enter their password (the same one used to access the Remote Desktop Connection sessions). Users will then be able to select the system to "remember" the printer password.