MSD IT High Compliance system

Fact sheet

The MSD IT High Compliance System (HCS) is a service for Clinical Trials Units (CTUs) and Medical Division Departments or Units who need to securely access critical applications and manipulate and temporarily 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; this user is the 'Data Manager' of the project. The group leader will be considered the 'Data Owner' and they may also nominate themselves as the 'Data Manager', who 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

You can reset your password while you are connected to the Remote Desktop system:

Hit 3 keys on your keyboard at the same time: Ctrl + Alt + Delete

1. You will be presented with a short list of tasks, select 'Change a password'.
2. Input your old password, and your new password (twice).
3. Click on the arrow pointing to the right.
4. In the next window, click 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 reasons.

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 (OpenText/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 application 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. Logout

The safest way to come out of the HCS is to close and save all your open files, then logout. To this effect, we have created a shortcut on the desktop named "Logout".

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.

Closing the HCS window using the 'X' button at the top right of the window is risky as your session will not close properly.

If you simply want to lock your session and come back to it later, use the "Lock" icon. This will activate the screen saver, and you will be required to input your password to unlock your session. It is always a good idea to save all your files before locking your session.

8. Lock your session

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 it is always a good idea to save all your files before locking your session.

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.

9. Where are the programs that you can use?

The applications and programs are accessible from the Start menu. Click on the Window icon at the bottom left of the desktop to activate the Start pane. In the Start pane you will get a down-arrow at the bottom left of the pane. Clicking on it will reveal all the applications installed on the HCS server.

To come back to the desktop without starting a program, click on the Desktop.

If you cannot find an application on the Start tile, use the magnifying glass at the top right of the Start pane, type the name of the tool / program / application that you are looking for. You should get a list of possibilities in return. Right-click on the one you want to activate and select 'Pin to Start'. This will produce a shortcut for it on the Start pane.

10. Microsoft Office

The version of Microsoft Office programs is Office 2021. If you find some tasks difficult to carry out in this new version, a quick search online using Google or other online search engine should give you the assistance you need. In addition, colleagues around you might know a few tricks that will get you going quickly.

11. Customising your desktop

If you want to change the colour of the desktop background, right-click on the Desktop and select 'Personalize'. In the bottom row of icons, you will find 'Desktop Background'. Click on it. In 'Picture location' near the top of the window, click on the down arrow, and select 'Solid colors'. Select the background colour that you want, and then click on 'Save change'.

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 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 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.

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 14), with possible data loss.

17.   File transfer in and out of the system

Files can be transferred into or out of the HC system via a special interface available from within a Remote Desktop Connection session in the HCS, using the 'File Transfer In' and 'File Transfer Out' utilities. For this purpose you have a network drive named the T drive inside the HCS, and another T drive on the standard MSD IT/OpenText (Novell) system. It is important to remember that the T drive provided by the standard MSD IT system is not as secure as the T drive inside the HCS. Files should be kept on the standard T drive 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/OpenText (Novell) file system put your files inside the folder named with your username in your T drive.
2. In the Remote Desktop session open the File Transfer In application (icon with a green left pointing arrow over a flash stick)
3. For security purposes you will need to re-enter your High Compliance password. If you enter the password incorrectly the application will close.
4. You will be presented with the list of files that are ready to be transferred. Below the list you should enter the reason for the transfer. The manager of the project will receive a notification of all the transfers. When ready, press enter and then enter Y to confirm.
5. You will then need to enter your regular MSD username and password
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 blue right facing arrow on a status bar.)
3. For security purposes you will need to re-enter your High Compliance password. If you enter the password incorrectly the application will close.
4. You will be presented with the list of files that are ready to be transferred. Below the list you should enter the reason for the transfer. The manager of the project will receive a notification of all the transfers. When ready, press enter and then enter Y to confirm.
5. You will then need to enter your regular MSD username and password
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 your standard T into your standard H drive or any other shared drive or local filesystem.

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

18.   Maintenance of the system

In order to maintain the system with the most up-to-date applications and security patches, the servers may be rebooted during a 2 hour window between 3:00 am and 5:00 am without warning, any day of the week. For this reason files should not be left open overnight.

19.   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 the new HCS system. A local IT support officer might be required to arrange for the printer to be connected to the system.

You can access the printer configuration by double-clicking the icon "Devices and Printers" on the desktop.