

Recommendations for Hardware & Network Settings



for _____

Date: _____

This lists the requirements from Incisive Medical Systems and also recommendations from our experience.

It is not the responsibility of Incisive Medical Systems to install, adjust or maintain hardware, networks, peripheral devices or their related software.

Global	Checked ✓	By
1. Operating System on the workstations to be Windows XP Pro, Windows Server 2003 (2008), Vista Business or Windows 7 Professional. Not 95, 98, Me, XP Home, Vista Home or Windows 7 Basic or Home. (It is preferable to use the same OS on all workstations). Can be 32 or 64 bit edition.	<input type="checkbox"/>	
2. All current Service Packs for the Operating System and updated drivers for internal and external hardware devices to be sourced and loaded	<input type="checkbox"/>	
3. Full contact details supplied of all contractors and sub-contractors including after-hours numbers and their job specifications and responsibilities.	<input type="checkbox"/>	
4. All workstations to have screen-saver function (with password) turned on where patients are able to get access (confirm with Practice Manager/Administrator)	<input type="checkbox"/>	
5. All Power Management functions that could cause the network adapter to become inactive (eg hibernate) to be turned off, including laptops when on AC power mode.	<input type="checkbox"/>	
6. All computers and devices should be externally labeled with their network name or address.	<input type="checkbox"/>	
7. Remote access software to be installed and the connection tested with Incisive Medical Systems. Accepted options are – Terminal Server (Remote Desktop), Citrix Metaframe or TeamViewer.	<input type="checkbox"/>	
8. VPN Client software and login settings to be provided to Incisive (if required)	<input type="checkbox"/>	
9. If internet access is available, ensure that access to ftp sites is enabled.	<input type="checkbox"/>	
10. Provide document of Remote Access settings including any IP address, login, password, port numbers	<input type="checkbox"/>	
11. Provide details of directory structures used by health messaging applications	<input type="checkbox"/>	
Network		
12. Incisive to have a computer or domain User account created with the following rights: <ul style="list-style-type: none"> • Member of the Remote Access group • Member of Domain or Local Administrator group (if Local, login account access needs to be provided on each workstation) Use 'Incisive' as the login name and then inform Incisive of the password you have allocated the account.	<input type="checkbox"/>	
13. The computer account for every User must have read, write, create & modify permissions for files in the local application directory (\Spmwin) and also the root and subdirectories of the data directory. Every User must also be able to 'read' the Windows Registry	<input type="checkbox"/>	
14. A 'Shared' directory with read/write rights for all Users must be provided on the server and accessible by all workstations. The directory will normally be the Data subdirectory under the SPMWIN directory.	<input type="checkbox"/>	
15. Roaming Profiles are strongly not recommended. If used at all, they must be set to allow only one occurrence of the login on the network.	<input type="checkbox"/>	
16. Network logins and workstation names are to be documented, including Administrator, and kept onsite by the Practice manager/Administrator	<input type="checkbox"/>	
17. Opportunistic Locking needs to be turned OFF where Win NT is on a workstation and Win 2000/XP/2003 is on the server	<input type="checkbox"/>	
18. Preference for all network cards to be the same brand. If not, check they are configured to	<input type="checkbox"/>	

manufacturers' recommendations and optimized for the hub/switch.		
19. Ensure network cards have the power-saving options turned OFF	<input type="checkbox"/>	
20. Printers to be workstation (not user) specific and available for all network logins.	<input type="checkbox"/>	
Server		
21. Server drive(s) to be accessible (with read/write abilities) from the Remote Access computer	<input type="checkbox"/>	
22. Report of UNC and drive/directory mapping settings that are available to us	<input type="checkbox"/>	
Workstations		
23. Enable Read/Write/Modify rights to the local SPMWIN directory and subdirectories	<input type="checkbox"/>	
24. Network card and System power-save functions to be disabled	<input type="checkbox"/>	
25. Screen resolution to be set to 1024x768 (or higher)	<input type="checkbox"/>	
26. Screen colours to be 32000 or 64000 colours	<input type="checkbox"/>	
27. Menu animation, and all non-essential graphical views to be turned off (Control Panel – Display – Effects)	<input type="checkbox"/>	
28. Web effects disabled, all extensions shown	<input type="checkbox"/>	
29. Numlock to be turned on at boot-up	<input type="checkbox"/>	
30. Regional settings to be English (NZ) or English (Aust). Date format to be dd/mm/yyyy	<input type="checkbox"/>	
31. Reduce the opening of files at startup of the computer to the minimum possible	<input type="checkbox"/>	
32. Time & Date settings of workstations to be set by the server. Server time to be accurate	<input type="checkbox"/>	
33. List of Network protocols used and the IP addresses for each workstation/device	<input type="checkbox"/>	
34. If Windows Server 2003 or 2008, allow the SPM_*.exe files to be excluded from 'Data Execution Prevention' (C/Panel – System – Performance – Advanced – DEP)	<input type="checkbox"/>	
Database - Microsoft Access		
35. Go into the ODBC drivers and set the 'Timeout' at 1000. Change this setting for ALL Access drivers installed.	<input type="checkbox"/>	
36. Go into the ODBC drivers and set the 'Buffer' at the recommended setting for the amount of memory on the computer. Search MSDN Knowledge Base Article 154384. Use a minimum of 10240	<input type="checkbox"/>	
Database - Microsoft SQL Server		
37. If SQL database, use Microsoft SQL Server 2000, 2005, or 2008; Express, Standard or Enterprise editions; fully checked for licences.	<input type="checkbox"/>	
38. SQL Enterprise Manager (or Management Studio) to be loaded onto, or available to the account login provided to Incisive for Remote Access	<input type="checkbox"/>	
39. The Login and Password for the SQL Server database used by the Incisive application is to be the ones provided by Incisive.	<input type="checkbox"/>	
40. System DSN - ODBC drivers for SQL to be configured to use Named Pipes or TCP/IP to access the Incisive SQL database from each workstation.	<input type="checkbox"/>	
41. If using a 64bit OS on the workstation, ensure the 32bit version drivers are used to connect to the database (\\Windows\\syswow64\\odbcad32.exe). See Microsoft Article: 942976	<input type="checkbox"/>	
42. Ensure the version of the ODBC driver correctly matches the version of SQL	<input type="checkbox"/>	
43. Enable SQL Browser if using Dynamic TCP/IP address	<input type="checkbox"/>	
44. SQL Authentication (not Windows Authentication) is to be used as the method of verifying the Login ID	<input type="checkbox"/>	
45. Optional – if server is dedicated to SQL, turn on the /3GB switch in Windows – System - Environment	<input type="checkbox"/>	
Terminal Server/Citrix		
46. On the application server, check or add Citrix=True to the [Workstation] section in the SPM.INI file	<input type="checkbox"/>	

47. Configure Remote Desktop Client: - 16 bit colour & Full screen size (Display) - Unselect all background images, effects & themes (Experiences) - Unselect 'Printers' option (Local Resources)	<input type="checkbox"/>	
48. Set up printers as per Incisive document 'Setting up printers.doc'	<input type="checkbox"/>	
49. If scanning, use a WAN capable scanner or purchase RemoteScan software from www.remote-scan.com (or similar software)	<input type="checkbox"/>	
50. Provide Incisive with a TS/Citrix login and access to Terminal Server Manager application.	<input type="checkbox"/>	
51. Recommend minimum of 512MB of memory allocated per User session.	<input type="checkbox"/>	
52. Allow User access to Task Manager (or Citrix equivalent)	<input type="checkbox"/>	
Backup		
53. Make sure the correct data and image files are being backed up. Refer to Tech Sheet.	<input type="checkbox"/>	
54. Produce a document showing backup settings/scheduling. Keep onsite.	<input type="checkbox"/>	
55. Instruction of staff in backup, tape rotation, tape security and data restoration procedures	<input type="checkbox"/>	
56. Instruction of staff in how to review backup log report each day and action to take if failed.	<input type="checkbox"/>	
57. Backup tapes for each day of the week and one monthly	<input type="checkbox"/>	
58. Where possible, have an automated daily copy of data directory to a second workstation (for emergency continuation in event of server failure)	<input type="checkbox"/>	
59. Larger systems to have capability to backup a 'file in use' (still open)	<input type="checkbox"/>	
60. Have agreement with Practice/Hospital regarding response time for restore from backup.	<input type="checkbox"/>	
Printers		
61. Set up printers as per Incisive document 'Setting up printers.doc'	<input type="checkbox"/>	
62. Latest printer drivers to be sourced from the appropriate website and installed	<input type="checkbox"/>	
63. Complete Windows test print at every workstation for each printer accessed	<input type="checkbox"/>	
64. Supply sufficient paper and labels to allow start up	<input type="checkbox"/>	
65. Set default paper tray in printer driver to be A4, plain paper feed tray NOT 'Auto-select'	<input type="checkbox"/>	
66. Printer resolution set to 600dpi or less (for faster printing)	<input type="checkbox"/>	
67. Thermal label printer paper settings to Landscape	<input type="checkbox"/>	
Scanning		
68. Latest TWAIN driver for the scanner and OS to be downloaded and installed	<input type="checkbox"/>	
69. Test scanner functionality. Use 3 rd party application such as IrfanView (free download from http://www.irfanview.com) to test TWAIN functionality. Don't rely on Microsoft scanning options.	<input type="checkbox"/>	
70. Turn OFF launch of specific events when scanning. -> Control Panel – Scanners & Cameras	<input type="checkbox"/>	
Anti-virus		
71. Virus checker enabled but to exclude files in \SPMWIN and the database files	<input type="checkbox"/>	
72. Procedure in place for the regular updating of virus data files	<input type="checkbox"/>	
Training		
73. Staff to be trained in power up and shut down of computer as well as logging on to the network	<input type="checkbox"/>	
74. IT manager, Practice manager or person responsible for computing to be instructed in shutting down the server and re-powering as well as purging of print jobs.	<input type="checkbox"/>	
Other		
75. All software installed and drivers used to be clearly labeled for the devices they are specific or relevant to and to be stored neatly away.	<input type="checkbox"/>	

76. Report showing location of legacy databases and program files	<input type="checkbox"/>	
77. If required, provide a 'Test' environment to allow training or testing without comprising the main production system. Call Incisive to discuss further		

Every practice and hospital have different configuration of hardware, network and software. In all instances, if you are unsure please call the Incisive Helpdesk to discuss the matter.