1. Ensure that project prerequisites have been carried out:
    1. Gather the relevant IP details from the customer for each individual server / installation site (e.g. Bristol, Exeter and Plymouth).
    2. Add an appropriate DNS entry to the ISEEU Global infrastructure held by 4U Hosting for each individual server / installation site (e.g. Bristol, Exeter and Plymouth).
    3. Setup an email forwarder in the ISEEU Global email infrastructure held by Google for each individual server / installation site (e.g. Bristol, Exeter and Plymouth).
    4. Request an account with MediaBurst on behalf of each individual server / installation site and register the IP address of each server to enable them to send SMS messaging via the ISEEU Global MediaBurst account (e.g. Bristol, Exeter and Plymouth).
2. Insert Red Hat 6 DVD in the drive and boot from it.
3. At the Red Hat Enterprise Linux 6.0 menu select the first option "Install or upgrade an existing system" and press "Return".
4. Choose "Skip", to bypass the media test.
5. At the Red Hat Enterprise Linux 6 splash screen click "Next".
6. Choose English(English) as the installation language and click "Next".
7. Choose United Kingdom for the keyboard layout and click "Next".
8. Select Basic Storage Devices and click "Next".
9. A warning box will pop-up, click "Re-initialize all".
10. If you know the hostname of the system then enter it in the box, otherwise leave it as default, it can be set after the installation. Click "Next". (Hostname pattern = crr-12345.iseeuglobal.com)
11. Select Europe/London for the timezone, the "System Clock uses UTC" box should be checked and click "Next".
12. Enter a root password, then re-enter it in the box below. Click "Next".
13. For the installation type, select "Use All Space", then check "Encrypt System" and "Review and modify partitioning layout", then click "Next".
14. Highlight the VolGroup (e.g. vg_crr12345) and click "Edit".
15. In the "Edit LVM Volume Group" window highlight lv_root and click "Delete".
16. In the "Edit LVM Volume Group" window highlight lv_home and click "Delete".
17. Click the "Add" button
18. In the "Make Logical Volume" box select / for the mount point, ext4 for the file system type, leave the Logical Volume Name as default and enter 10240 for the size. Leave Encrypt unchecked. Click "OK".
19. Repeat the above steps 16 and 17 for /var and /tmp mount points with the same parameters. Then repeat again for /home but assign all remaining space to it.
20. Once done, click "OK".
21. Review the partition information and if correct, click "Next".
22. If a format warning box should appear, click "Format".
23. Enter a passphrase for the encrypted partition in the box that appears, enter it again in the confirm space and click "OK".
24. Click the "Write changes to disk" button in the window that pops up.
25. Tick "Use Bootloader Password" and in the popup box enter a password (same as root password). Click "Next".
26. Make sure "Basic Server" is selected and also select "Customize Now". Click "Next".
27. Select the following options and then click "Next":

Package Type	Package	Optional Packages	
		Check	Uncheck
Base System	Base (60 of 108)	logwatch	abrt-addon-ccpp abrt-addon-kerneloops

~~Do not~~ Check/uncheck Install boot loader on /dev/sda

			abrt-addon-python abrt-cli abrt-plugin-sosreport sysstat
Servers	None		
Web Services	None		
Databases	MySQL Database Server (0 of 2)		
System Management	None		
Virtualisation	None		
Desktops	Desktop (13 of 17)		
	Desktop Debugging and Performance (1 of 7)		abrt-desktop
	Desktop Platform (0 of 6)		
	General Purpose Desktop (37 of 49)		
	Graphical Admin Tools (8 of 15)		
	X-Windows System (8 of 9)		
Applications	Internet Browser (3 of 3)		
Development	Additional Development (37 of 102)		libcgroup-devel
	Development Tools (16 of 43)		
	Server Platform Development		
Language	English UK Support		

26. The packages will now be installed. When the system prompts you to reboot do so.
27. When the system reboots, you will be asked for the LUKS password.
28. The system will boot to a Welcome screen. Click "Forward".
29. Agree to the licence agreement and click "Forward".
30. You will see a "Set Up Software Updates" screen, click "Forward".
31. You cannot set up software updates at this time because you are not connected to a network yet. This can be done after the system is installed.
32. At the "Finish Updates Setup", click "Forward".
33. Now you will need to create the iseeuglobal user.
34. In the Username field, enter iseeuglobal. Full name should be entered as "ISEEU Global Standard User Account" and enter a password in the password field (same as the root password). Confirm that password in the confirm password field. Click "Forward".
35. Set the date and time of the system and click "Forward".
36. A message box stating there is insufficient memory to configure kdump may appear, click "OK".
37. Click "Finish" at the kdump screen.
38. The system will now boot to a login prompt.
39. Login as the iseeuglobal user.

The next step is to enable the network adapter. To obtain an IP address etc you will need to consult your system administrator.

40. System/Preferences/Network Connections, highlight the adapter (e.g. eth0) and click "Edit".
41. Check "Connect Automatically" and click "Apply".
42. Enter the root password and click "Authenticate".
43. Close the Network Connections window.

The next step is to remove software that does not need to be installed.

45. Open a terminal window and switch user to root (su -).
46. Now enter the following commands:
    yum erase httpd (removes 2 packages)
    yum erase crash (removes 2 packages)
    yum erase kexec-tools (removes 2 packages)
    yum erase libvirt-client (removes 4 packages)
47. Close the terminal window.
48. System/Administration/Firewall. Authenticate when prompted.
49. Add "Secure WWW (HTTPS)" and amend other protocols as required for any remote management.
50. Click "Apply" to save your changes and click "Yes" on the popup to override existing settings. Close the firewall config tool.
51. System/Administration/RHN registration. Authenticate when prompted. At the Registration screen, click "Forward".
52. At the Update Location screen, leave as defaults then click "Forward".
53. At the Account Information screen, enter the ISEEU Global Red Hat Network account username and password and click "Forward".
54. Change the System Name to reflect the hostname and a meaningful customer or site location name e.g. crr-12345 – Customer_Hospital. Click "Forward".
55. At the review System Subscription Details screen, ensure that the server is subscribed to an updates channel e.g. rhel-i386-server-6. Click "Forward" and at the Finish screen click "Finish". NOTE: wait for a few minutes before instigating any software updates.
56. Check that the new server appears in the Systems Overview screen on the Red Hat Network portal for ISEEU Global.
57. Start a terminal window and maximise the screen. Switch to the root user (su -) and type "yum update". Download and apply updates. Run the "yum update" command until told there are no further packages to update.
58. The ServeRAID M1015 GUI software is installed from ibm_sw_msm_8-17-21_linux_32-64.zip, extract the zip file into a folder on the desktop and further extract the .tar.gz file that is created. Change into the sub-directory named "disk" and "chmod 777 *" and "chown root:root *" then run "./install.sh -s" (which installs in the standalone mode as opposed to the network-based mode). You can ignore the error message "scriptlet failed, exit status 1" as this appears to be caused by failing to find an snmp config file.
59. The ServeRAID GUI software is installed under Applications/System Tools/MegaRAID Storage Manager StartupUI. As the UI starts, if prompted for a valid IP address, click "OK" then in the IP Address window type 127.0.0.1 and click "Discover Host". This will populate the Remote Servers List with the fully qualified host name. Select the server and authenticate as root to enter the ServeRAID Manager GUI.

60. Unpack the ibm_utl_sraidmr_megacli-8.00.48_linux_32-64.zip file, creating a folder named linux. Under the folder named linux, the ServeRAID M1015 command line tools are installed from MegaCli-8.00.48-1.i386.rpm by right-clicking and using Package Installer. Authenticate when prompted. Please note, the Lib_Utils-1.00-09.noarch.rpm file is unnecessary as this package is installed during the ServeRAID GUI installation.
61. The command line tools are installed under /opt/MegaRAID/MegaCli and can be tested with the command "./MegaCli -ShowSummary -aAll" or "./MegaCli -PdList -aAll"
62. Remove any extraneous or unwanted folders from the Desktop.
63. As root, copy the RAID monitoring script "Raid_Check_Script" into /etc/cron.daily then "chown root:root" and "chmod 755".
64. Use vim to edit the file; change the "Subject" entry to something meaningfully related to the site e.g. "Bristol_Hospital_RAID_Status". Test by running the script and ensure that an email is received with the current status information.
65. The installation of Courier can now proceed. Begin by patching the Linux OS to date as in step 57 above.

START: 66. Copy the installation folder to the iseeuglobal users' Desktop and rename the folder to "current"

67. Use "chown -R root:root current" and "chmod -R 777 current" to change ownership and permissions on the installation folder.

68. "cd current" and run the install script with "../courier4_0_install_script"
69. When prompted, enter the existing LUKS passphrase and then enter an ISEEU specific backup passphrase "ungorowarlock123" into Key Slot 1. Add addtn passphrase labolgreesi123
70. When prompted, enter the server DNS name (bri.iseeuglobal.com)
71. The MySQL configuration script will prompt for the root password before setting a MySQL password. When prompted to set a root MySQL password, answer "Y" and enter the root password, minus the numeric suffix with the two component words capitalised e.g. "ungorowarlock123" becomes "UngoroWarlock".
    1. Remove anonymous users "Y"
    2. Disallow remote login "Y"
    3. Remove test databases and access "Y"
    4. Reload privilege tables now "Y"
72. Next step moves and unpacks the source files – press "Return" to begin.
73. Next step moves the layout file and compiles Apache – press "Return" to begin.
74. Next step compiles PHP and applies the configuration file – press "Return" to begin.
75. Next step is to move and unpack the Courier code – press "Return" to begin.
76. Next step creates the blank database for Courier – press "Return" to begin. When prompted, enter the MySQL root password (UngoroWarlock).
77. Next step creates the required application directories – press "Return" to begin.
78. Next step copies the required configuration files into the application directories – press "Return" to begin.
79. Next step creates a server key file – press "Return" to begin.
80. Next step creates a certificate request file – press "Return" to begin. Enter the following details when prompted:
    1. Country Name: GB

2. State or Province: North Somerset
3. Locality : Bristol
4. Organisation: ISEEU Global Limited
5. Organisation Unit: Information Technology
6. Common Name: use the server host name (bri.iseeuglobal.com)
7. Email Address: technical@iseeuglobal.com
8. Challenge Passwd: leave blank
9. Optional Company Name: use the installation site (Bristol Hospital)

81. Next step generates a 365-day self-signed certificate to enable the server and services to come up in a live state prior to installing a full CA purchased certificate – press "Return" to begin. Make a note of the 2 filenames that require editing:
    1. hostname.key (bri.iseeuglobal.com.key)
    2. hostname.crt (bri.iseeuglobal.com.crt)
82. Next step installs the IonCube software – press "Return" to begin.
83. Next step installs the required GPG keys for GridCard upload – press "Return" to begin.
84. Next step halts any unnecessary services and performs an initial system cleanup – press "Return" to begin. This step can look somewhat "ugly" as services for removal may not yet be running.
85. Next step lists the Courier config files for editing – press "y" to begin.
86. First file is the Courier config file localcfg.inc – press "Return" to begin. All fields in UPPERCASE need to have their values updated with the server / site specific details.
    1. $user - "root"
    2. $password - "UngoroWarlock"
    3. _SYSNAME_ - "crr-75008"
    4. _BASEURL_ - "https://bri.iseeuglobal.com"
    5. _ADMAIL_ - "Bristol-Courier-Service@iseeuglobal.com"
    6. _SMSUNAME_ - "bri.iseeuglobal.com"
    7. _SMSPWD_ - "Y74bj8E"

Save the file with "wq"

87. Second file is the archive config file – press "Return" to begin.
88. Exit from the file editor with "q"
89. Third file is the SSL config file – press "Return" to begin. All fields in UPPERCASE need to have their values updated.
    1. ServerName bri.iseeuglobal.com:443
    2. SSLCertificateFile "/etc/httpd/extra/bri.iseeuglobal.com.crt"
    3. SSLCertificateKeyFile "/etc/httpd/extra/bri.iseeuglobal.com.key"
    4. SSLCertificateChainFile <only update this if using a NON Comodo certificate>

Save the file with "wq"

90. Fourth file is the Logwatch config file – press "Return" to begin. Need to edit:
    1. MailTo = technical@iseeuglobal.com

2. MailFrom = Bristol-Courier-Service
3. Detail = Med

Save the file with "wq"

91. The installation will now prompt you to reboot. Answer "y" and press "Return"
92. Post install cleanup and testing should now be carried out. Begin with starting a local browser pointed at https://localhost (ignore the certificate error, adding an exception). You should get back a Courier Login Screen.
93. Login using the credentials:
    1. Username – iseeuglobal
    2. Password – scherZo

Please Note: The SMS 2nd FA will be sent to Tony's Mobile (07796 613566)

94. Create the 3 standard Admin accounts for ISEEU Global staff (tony.donoghue, steve.clements & david.nunn) BUT DO NOT ADD THEM TO THE RECIPIENT ADDRESS BOOK.
95. Logout and do not use the iseeuglobal account for any further work. Instead, login under your own administrative account. Perform a basic service test by publishing to yourself:
    1. /etc/httpd/httpd.conf
    2. /etc/httpd/extra/httpd-ssl.conf
    3. /etc/httpd/extra/<certificate .crt file>
    4. /etc/httpd/extra/<server certificate .key file> (NOTE: you need to "su –" in a terminal window and make a copy of this file plus "chmod 777" as the original .key file is readable only by root. Once the copy is published, DELETE THE COPY)
    5. /etc/httpd/extra/comodo.ca-bundle
    6. /usr/local/lib/php.ini
    7. /home/httpd/htdocs/global/localcfg.inc
    8. /usr/share/logwatch/default.conf/logwatch.conf
96. To complete the basic test, login to Courier USING A SEPARATE PC and download the files published in the previous step. Also check that the audit trail confirmation mesage is sent out and received once the files are downloaded.
97. Ensure that the daily Logwatch process runs and that the report is mailed out as appropriate. Run the command manually in a terminal window as the root user via "/etc/cron.daily/0logwatch".
98. Finally, conduct full system testing by following the standard Courier testing procedure.
99. Before shipping the server to the customer site, ensure the following pre-requisites are carried out:
    1. Cleanup the Desktop, removing the installation files and empty the recycle bin.
    2. Apply the correct customer-site IP configuration.
    3. Ensure the proper SSL certificates have been installed.
    4. Licence the server by encrypting the localcfg.inc file using IonCube.

* Basic configs (such as max filesize etc). / IP setup.
* Database backup.
* Email + SMS templates.
* Encode localcfg.inc
* setup risk register
* Test functionality + restore database.