Joining the NHS Scotland Video Conferencing Service
“The Implementation Cook Book”

Version 1.2

August 2011

Unrestricted Version without Firewall Configurations

Classification: **None**

1. Purpose of the Document

The purpose of this documents it to provide an easy to implement guide to migrate or establish local video conferencing services that comply with the national standards, communicate over N3 and can utilise the national VC infrastructure.

The document does not set out to provide a full set of options, but aims to provide a workable solution that can be easily implemented.

2. Summary of the NHS Scotland Video Conferencing Standards

2.1. Quality of Service

To achieve Quality of Service for video services, network traffic is marked at the N3 router, based on source or destination IP address. Video conferencing can be identified and tagged as Assured Forwarding number 4 (AF4) of the six layer model.

QoS on N3 is only effective across the N3 network (i.e between N3 routers) and does not extend to end point devices on the LAN or non-N3 routers within COINS. Extension of QOS into the LAN environment can be achieved by setting up VLAN's within the Health Board network to separate video devices from voice and data networks. These VLAN's should adopt QoS wherever possible; this could be by trusting the N3 marked packets, or re-marking locally to local standards.

2.2. IP Addressing

The IP subnet reserved for video services is 10.247.64.0/18 (10.247.64.0 to 10.247.127.255)

Applications for video addresses should be made to nisgtelecom.nss@nhs.net

2.3. Firewall Recommendations

A range of methods and products are available that allow traversal of NAT and firewall boundaries in a secure and timely manner. The preferred solution to overcome these problems will depend upon the local site's security policy, IP addressing policy and choice of firewall products.
It is planned that for VC, the DMZ deployment or H.323 aware firewalls can be adopted both centrally at the data centre and locally at the Health Boards. When these solutions aren't appropriate, border negotiation devices should be considered.

DMZ Port Requirements -

- Firewall at all sites to allow all ports to/from 10.247.64.0/18 on the DMZ interface, or,
- Firewall at all sites to allow the ports shown to/from 10.247.64.0/18 on the DMZ interface.
- Firewalls to deny access between their DMZ and their local/hosted services

2.4. Gatekeeper Hierarchy

Gatekeepers within NHS Scotland will be arranged in a hierarchy with each gatekeeper only knowing its parent and child gatekeepers as well as any directly registered endpoints. The central NHS Scotland gatekeeper will be linked to the JANET network to provide onward routing.

2.5. Dial Plan

End points should be programmed with a minimum of the last 9 digits of the E164 address. This will ensure that E164 numbers displayed will operate across all health board areas in Scotland. The master gatekeeper will be programmed to add or remove the additional 6 digits that uniquely identifies NHS Scotland (004405) to external calls.

The Dial Plan is detailed below.

Table 1 The Dial Plan

	UKERNA Assigned			**Regional or National Gatekeepers** To be programmed into end points	
	International Prefix	Country Code	Zone Prefix	Gatekeeper Prefix	Extension
GDS Number for NHS Scotland	00	44	05		
Ayr & Arran	00	44	05	513	yyyyyy
Borders	00	44	05	514	yyyyyy
Dumfries & Galloway	00	44	05	515	yyyyyy
Fife	00	44	05	516	yyyyyy
Forth Valley	00	44	05	517	yyyyyy
Grampian	00	44	05	511	yyyyyy
Greater Glasgow & Clyde	00	44	05	518	yyyyyy
Highland	00	44	05	510	yyyyyy
Lanarkshire	00	44	05	519	yyyyyy
Lothian	00	44	05	520	yyyyyy
Orkney	00	44	05	521	yyyyyy
Shetland	00	44	05	522	yyyyyy
Tayside	00	44	05	512	yyyyyy
Western Isles	00	44	05	523	yyyyyy
NHS24	00	44	05	524	yyyyyy
NSS	00	44	05	525	yyyyyy
Scottish Ambulance Service	00	44	05	526	yyyyyy
Golden Jubilee Nat Hosp	00	44	05	527	yyyyyy
Quality Improvement Service	00	44	05	528	yyyyyy

National Education for Scotland	00	44	05	529	yyyyyy
State Hospital	00	44	05	530	yyyyyy
NHS Health Scotland	00	44	05	531	yyyyyy

For example, an endpoint in Highland will have an E164 address programmed into the endpoint of:

510123456

Health boards will be required to educate users that the full external address would be:

004405510123456

2.6. H323 ID & URL Dialling

This field may be left blank or configured for local use as all calls will be routed using E164 addresses. When a call is made using a URL the domain name will be stripped by the VCS and the call routed using the E164 address.

If a user wishes to dial a URL it must be of the form

<9 digit E164 Address>@vc?.scot.nhs.uk where ? is the agreed board identifier (max 3 characters) used in the system name.

e.g. 512123456@vct.scot.nhs.uk for an endpoint in Tayside

For SIP only systems uniquely identified with an individual user (eg PC based systems) the recommended standard remains:

<NHSMail User Name>@vc.scot.nhs.uk

i.e joe.bloggs@vc.scot.nhs.uk for centrally registered Movi users

or joe.bloggs@vcY.scot.nhs.uk (where Y = board identifier)

The vc.scot.nhs.uk should be routable and should resolve to the appropriate VCS / SIP registrar.

3. Joining the IP Subnet

- Identify the sites on your network that require video conferencing access.
- For each site, estimate the number of hardware based video conferencing systems that you currently have.
- For each site, using the information above, establish the number of IP addresses you need to allow a reasonable degree of growth. Please do not over apply for addresses, as the available address range is small.
- Apply to National Services for you address allocation by e-mailing nisgtelecom.nss@nhs.net.
- For each N3 site complete the change request form (see Appendix 1) using the address allocation given, and adding in the site details. Completed forms should be emailed to nisgtelecom.nss@nhs.net.
- Please note that PC based video conferencing systems are not allowed onto the VC subnet. This is for dedicated, hardware based video conferencing systems only.

4. Internal Network Configuration

N3SP will route the VC Subnet to the local site Firewall. How the subnet is distributed throughout the site depend upon the site configuration.

While there are a number of options for deploying video conferencing with the organisation, the simplest is to establish a routable video conferencing VLAN. It is recommended that QOS is enabled.

5. Firewall Traversal

If the VLAN solution is adopted, it will be necessary to allow video data on the VC subnet to pass through the firewall. As the video network is for VC systems only some board have decided to allow all traffic on the VC address range (10.247.64.0/18,10.247.64.0 to 10.247.127.255) through the firewall.

Table 2 Firewall Rules – Open Configuration

Source IP	Source Port	Destination IP	Destination Port

Should tighter controls be required, the following is a list of rules currently identified. However please note that video conferencing is notorious for using non-standard ports. It should be anticipated that if this solution is adopted, a degree of testing and maintenance should be anticipated.

Table 3 Firewall Port Configuration – Restricted Configuration for Tandberg / Polycom Systems

Source IP	Source Port	Destination IP	Destination Port

If using Lifesize systems the following additional rules will be required

If you are using the central TMS server the following rules will also be required.

Table 4 Firewall Rules Required to Support TMS Management System

Source IP	Source Port	Destination IP	Destination Port

It is recommended that where firewalls support H323 / SIP awareness, this is not enabled.

6. Gatekeeper Configuration

If a gatekeeper[1] is utilised within the health board set up, this should be set up to link to the national gatekeeper. This should be undertaken in conjunction with the current maintenance provider, NuVideo and NISG.

Gatekeepers should not be neighboured with other health boards as a strict hierarchy is in place.

Where no gatekeeper currently exists, consideration can be given to registering video conferencing endpoints with either the central gatekeeper or a partnering health board.

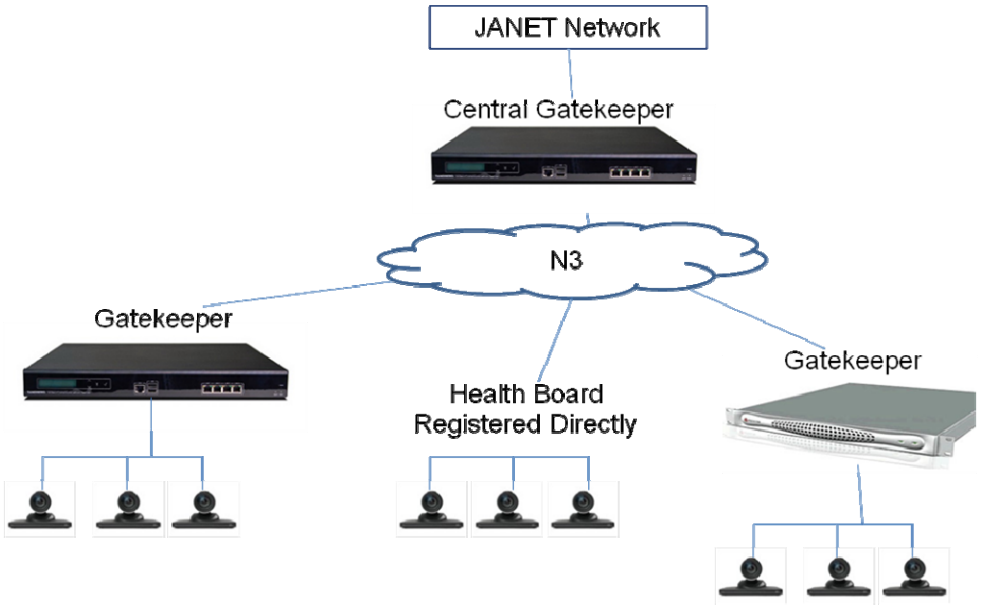
Considerations for this are as follows:

- ISDN connectivity will still be required for connection to systems outwith the N3 network
- If ISDN breakout is required, devices must be registered on the same gatekeeper as the ISDN Gateway
- ISDN breakout is not currently provided as a central service on the national gatekeeper.
- Health boards such as NHS Highland, NHS Grampian and NHS Lothian may be able to provide gatekeeper / gateway services through local agreement.
- The impact on the number of concurrent call licences on the gatekeeper should be considered. If this is high, a more appropriate solution may be the purchase of a local gatekeeper.

For advice on Gatekeeper configuration, please contact hazel.archer@nhs.net

[1] A Gatekeeper is a network device that provides addressing service for H.323 (Internet-based) videoconference clients. It may also be configured to impose network bandwidth restrictions and establish dialling rules. Registration by the videoconference client usually takes place when the client is started; the address of the gatekeeper is put into the client's configuration. Use of a gatekeeper allows a videoconference device to "dial" another device using the videoconference address rather than an IP address (which could be changed by DHCP).

Figure 1 Gatekeeper Hierarchy



7. Video Conferencing Dial Plan

The video conferencing dial plan is based on a hierarchy where each gatekeeper knows the location of the systems registered to it and the gatekeeper above it. Traffic is routed by way of the E164 address. The E164 address is made up of a number of parts. Within NHS Scotland, the agreed dial plan is as follows:

International Prefix	Country Code	Zone Prefix	Gatekeeper Prefix	Extension
00	44	05	5xx	yyyyyy

Within NHS Scotland, it has been agreed that only the last 9 digits of the full E164 address need to be used for endpoint configuration and dialling. Traffic leaving the NHS Network will be automatically prefixed with 004405.

Gatekeeper prefixes are allocated by NISGTelecom. 6 digit extension numbers are allocated by health boards.

Consideration should be given to adopting an appropriate dial plan within the Health Board. Options include:

- Using the last 6 digits of existing ISDN extension numbers
- Using a site identifier, followed by ISDN DDI numbers
- Sequential numbering (if ISDN DDI is not required)

If the health board contains more than one gatekeeper, this needs to be reflected in the dial plan. If required, advice can be provided from the project team. (Contact hazel.archer@nhs.net for details.)

8. System Naming Conventions

The name is used to identify endpoints appears in various places in the web interface of management system, and in the display of the video endpoint unit (so that you can identify it when it is in a rack with other systems). The system name is also used by management systems. We recommend that the systems are named in a way that allows you to easily and uniquely identify it.

The agreed naming convention for videoconferencing endpoints is as follows.

Healthboard.town.site.room

For example, a videoconferencing endpoint situated in the Conference Room at Aberdeen Royal Infirmary would be displayed in the following format;

NHSG.Aberdeen.ARI.Conference_Room

To avoid names of excessive length, health boards may use recognised abbreviations in the town.site.room section.

The healthboard section must be unique and should conform to the following table.

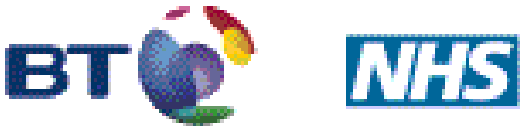
Table 5 Agreed Health Board Identifiers

Health Board	Identifier
Ayr & Arran	NHSAA
Borders	NHSBOR
Dumfries & Galloway	NHSDG
Fife	NHSFIF
Forth Valley	NHSFV
Grampian	NHSG
Greater Glasgow & Clyde	NHSGGC
Highland	NHSH
Lanarkshire	NHSLAN
Lothian	NHSLOT
Orkney	NHSORK
Shetland	NHSSHE
Tayside	NHST
Western Isles	NHSWI
NHS24	NHS24
NSS	NHSNSS
Scottish Ambulance Service	NHSSAS
Golden Jubilee Nat Hosp	NHSGJ
Quality Improvement Service	NHSQIS
National Education for Scotland	NHSNES
State Hospital	NHSSH
NHS Health Scotland	NHSHS
Board identifier – Max 6 characters must be unique and agreed by NSS **4 character names – may be allocated based on board cipher unless prior agreement between boards** e.g. NHSG.Aberdeen.ARI.Committee_Room_1	

9. Endpoint Configuration

Before proceeding with a full scale migration, it is recommended that a test system be configured using the settings described in Appendix 2. Using this test system, a range of calls should be made to systems across a number of health boards. These test calls should include both Tandberg and Polycom systems. When you are happy with the configuration, each endpoint in turn should be configured with its new IP address and E164 number. When updating the systems it is recommended that the configuration options detailed in Appendix 2 are applied to each system.

10. Appendix 1 Sample Change Request Form



Working together to deliver N3

All fields are mandatory.

Requestor Details :

Requestor Name : ???	**Requestor Telephone :** ???	**Requestor E-mail :** ???

Site Details :

SIN : ???	**National GP Practice Code :**	**Site Name :** ???	**Site Address :** ???
PCT/SHA :	**Authorised By Name :** John Potts	**Authorised by telephone :** 01312756687	**Authorised by e-mail :** John.potts@nhs.net

Request Details :

Please route subnet 10.247.xx.y/z to next hop (local Firewall) address 10.x.x.x.

Reason For Request :

Route Video Conferencing subnet into site.

Date and Time Required (Please note that these changes will be completed within 5 working days from the date of acceptance) :

ASAP

Please e-mail all completed forms to btn3ccc@bt.com and mailto:nisgtelecom.nss@nhs.net

11. Appendix 2 Suggested Endpoint Configuration for Tandberg MXP

Feature	Status	Reasoning	Instructions
System Name	Mandatory	System names will be displayed in online directories and should be standardised to allow for easy identification and searching.	From the unit's web interface select the following options: End Point Configuration>General>System Name>[Healthboard.town.site.unit] Healthboard section must conform to the agreed health board identifier outlined in Table 2.
Auto Answer	Mandatory, following risk assessment	To prevent unauthorised access to meetings, patient consultations etc the level of auto answer should be set following a risk assessment (see Appendix 4). Auto answer with Mic On should not be used.	From the unit's web interface select the following options: End Point Configuration>General>Auto Answer>[On + Mic Off or Off]
H323 Call Setup	Mandatory	Required to provide H323 dialling using the gatekeepers.	From the unit's web interface select the following options: System Configuration>H.323>Callsetup Mode>Gatekeeper
E164 Alias	Mandatory	To facilitate connection between health boards	From the unit's web interface select the following options: System Configuration>H.323>E164 Alias>[9 digit E164 Address]
H323 ID	Optional	This field may be left blank or configured for local use as all calls will be routed using E164 addresses. When a call is made using a URL the domain name will be stripped by the VCS and the call routed using the E164 address.	From the unit's web interface select the following options: System Configuration>H.323>H.323 ID>[leave blank]
Gatekeeper Setup	Mandatory	Setting required to use a gatekeeper	From the unit's web interface select the following options: System Configuration>H.323>Gatekeeper Discover>Manual System Configuration>H.323>Gatekeeper Address>[IP address / DNS name of gatekeeper] When registering with the central gatekeeper the DNS name vc.scot.nhs.uk should be used rather than an IP address. This registers the device with the cluster rather than a single gatekeeper.

Feature	Status	Reasoning	Instructions
Welcome Screen	Optional	Allows for the dissemination of useful information, such as helpdesk numbers, training information etc	Design the Welcome Screen being sure to include all relevant information in a suitably sized font. For best results the screen dimensions should be 704 x 480 pixels. Check that the image appears as expected on the units. From the unit's web interface select the following options: Endpoint Configuration>Files>Welcome Screen/Logo>Browse… Select the appropriate file and then click Endpoint Configuration>Files>Welcome Screen/Logo>Upload To check the file has uploaded: Click 'Welcome Screen/Logo' which should then open another page displaying the uploaded file. To enable display of the Welcome Screen/Logo as the first thing users see select the following settings: Endpoint Configuration>Menu>Welcome Menu>Off Endpoint Configuration>Menu>Selfview Welcome Picture>Off Endpoint Configuration>Menu>Logo>On
NTP (Network Time Protocol)	Optional	Endpoints may fail to register with gatekeepers if they do not have NTP turned on. Accurate time stamps are useful for troubleshooting and generating call detail records.	From the unit's web interface select the following options: System Configuration>IP>NTP Mode>Manual System Configuration>IP>NTP Address>[address of NTP server]
Gatekeeper Authentication	Optional	Enabling authentication on gatekeepers means that only authorised endpoints can register and place calls through them.	Refer to the gatekeeper manual for instructions as to how to set up authentication at that end. From the unit's web interface select the following options: System Configuration>H.323>Authentication Mode>Auto System Configuration>H.323>Authentication ID>[unique authentication ID] System Configuration>H.323>Authentication Password>[unique authentication password in double quotes, eg "Pa55w0rd"]

Feature	Status	Reasoning	Instructions
System Contact	Optional	Adding a system contact allows for easy identification of who is responsible for a VC unit. This contact could be responsible for co-ordinating bookings of the unit and/or for local troubleshooting should a fault occur.	From the unit's web interface select the following options: System Configuration>SNMP>System Contact>[Contact Name - Telephone Number]
System Location	Recommended	Setting a system location in the correct format will allows it to be included in the online directory mapping application being developed for SHOW.	From the unit's web interface select the following options: System Configuration>SNMP>System Location>[xx.xxxxxx yy.yyyyyy nnnnn] Where xx.xxxxxx is the latitude, yy.yyyyyy is the longitude and nnnnn is the area code for the unit's ISDN lines or gateway, as appropriate, each field must be the correct number of characters long and separated by a single space character eg: SNMP SystemLocation> 57.123456 -4.123456 01234
Startup Video Source to Main Cam	Recommended	When a unit is restarted it reverts to the main camera as the video source, helping to avoid support call relating to the wrong source being displayed.	From the unit's web interface select the following options: Endpoint Configuration>Presentation>Startup Video Source>Main Cam

Feature	Status	Reasoning	Instructions
Call Video Source to Main Cam	Recommended	Whenever a unit receives or makes a call it reverts to the main camera as the video source, rather than any external sources which may have been selected. This should ensure that the far-end participants see the room view, rather than say a black screen if previous users had left the system in 'Presentation' mode but turned the PC/laptop off.	From the unit's web interface select the following options: Endpoint Configuration>Presentation>Call Video Source>Main Cam
Presentation Start to Auto	Recommended (depending on clinical requirements for image quality)	Setting the Presentation mode to auto start reduces end-user confusion by removing menus.	From the unit's web interface select the following options: Endpoint Configuration>Presentation>Presentation Start>Auto
Presentation Source	Recommended	Ensuring the Presentation Source is set (normally to PC) ensrues that when the user users selects Presentation mode the unit will automatically start sending video from the default source.	From the unit's web interface select the following options: Endpoint Configuration>Presentation>Presentation Source>PC
Menu Administrator Password	Recommended	Setting a Menu Administrator Password prevents end-users altering settings on the endpoint.	From the unit's web interface select the following options: Endpoint Configuration>Security>Menu Administrator Password>[numeric PIN]
Allow Incoming Calls when In a Call	Recommended (for systems not using multisite)	Accepting an incoming call on a system without multisite, put one of the callers on hold. This causes confusion and disruption of the meeting.	Using the remote control for the system: Control Panel>General>Permissions>Allow incoming call when in a call>Off Alternatively using telnet, enter the following command: xconfig Conference AllowIncomingMSCall: Off

Feature	Status	Reasoning	Instructions
Web Snapshot	Optional – depending on outcome of auto answer risk assessment. Systems assessed to have auto answer off should have web snapshots off.	With Web Snapshot enabled it is possible to view the unit's current video source via the unit's web page, thus allowing enhanced diagnostics if users are reporting issues with video. Additionally, from version F9.0 of the software onwards, Web Snapshot can be use in conjunction with Camera Control on the web interface to remotely move the unit's camera.	For security reasons this change must be made locally to the unit using the remote control by: Call up the 'Welcome Screen' on the unit Select 'Control Panel' Select 'Administrator Settings' Enter a 'Menu Password' if required Select 'Video' Set 'Web Snapshot' to 'On' Select 'Save' to store the new setting Once you have enabled Web Snapshot navigate to Overview>Overview on the web interface, where you should now see a snapshot of the current video source which updates approximately once every 2-3 seconds. If required, Camera Control can also be accessed from this screen.

12. Appendix 3 Suggested Endpoint Configuration for Polycom HDX (Software Version 3.0.2-11176)

Feature	Status	Reasoning	Instructions
System Name	Mandatory	System names will be displayed in online directories and should be standardised to allow for easy identification and searching.	From the unit's web interface select the following options: Admin Settings>General Settings>System Settings>System Name>[Healthboard.town.site.unit] Click the Update button at the top of the web page. Health board section must conform to the agreed health board identifier outlined in Table 2.
Auto Answer	Mandatory, following risk assessment	To prevent unauthorised access to meetings, patient consultations etc the level of auto answer should be set following a risk assessment (see Appendix 4). Auto answer with Mic On should not be used.	From the unit's web interface select the following options: Admin Settings> General Settings>System Settings>Call Settings>Auto Answer Point-to-Point Video>[Yes] Click the Update button at the top of the web page. **AND** Admin Settings>Audio Settings> Audio Settings>Mute Auto Answer Calls>[tick] Click the Update button at the top of the web page.
H323 Call Setup	Mandatory	Required to provide H323 dialling using the gatekeepers.	From the unit's web interface select the following options: Admin Settings>Network>IP Network>H.323 Settings>Enable IP H.323>[tick] Click the Update button at the top of the web page.
E164 Alias	Mandatory	To facilitate connection between health boards	From the unit's web interface select the following options: Admin Settings>Network>IP Network>H.323 Settings> H.323 Extension (E.164) >[9 digit E164 Address] Click the Update button at the top of the web page.

Feature	Status	Reasoning	Instructions
H323 ID	Optional	This field may be left blank or configured for local use as all calls will be routed using E164 addresses. When a call is made using a URL the domain name will be stripped by the VCS and the call routed using the E164 address.	From the unit's web interface select the following options: Admin Settings>Network>IP Network>H.323 Settings> H.323 Name>[leave blank] If changed click the Update button at the top of the web page.
Gatekeeper Setup	Mandatory	Setting required to use a gatekeeper	From the unit's web interface select the following options: Admin Settings>Network>IP Network>H.323 Settings>Use Gatekeeper>[Specify] Admin Settings>Network>IP Network>H.323 Settings>Primary Gatekeeper IP Address>[IP address / DNS name of gatekeeper] Click the Update button at the top of the web page. When registering with the central gatekeeper the DNS name vc.scot.nhs.uk should be used rather than an IP address. This registers the device with the cluster rather than a single gatekeeper.
NTP (Network Time Protocol)	Optional	Endpoints may fail to register with gatekeepers if they do not have NTP turned on. Accurate time stamps are useful for troubleshooting and generating call detail records.	From the unit's web interface select the following options: Admin Settings>General Settings>Date and Time>Time Server>[Manual] Admin Settings>General Settings>Date and Time>Time Server>Primary Time Server Address>[address of NTP server] Click the Update button at the top of the web page.

Feature	Status	Reasoning	Instructions
Gatekeeper Authentication	Optional	Enabling authentication on gatekeepers means that only authorised endpoints can register and place calls through them.	Refer to the gatekeeper manual for instructions as to how to set up authentication at that end. From the unit's web interface select the following options: Admin Settings>Network>IP Network>H.323 Settings>Authenticate>[tick] Admin Settings>Network>IP Network>H.323 Settings>User Name>[unique authentication ID] Admin Settings>Network>IP Network>H.323 Settings>Password>[tick] Admin Settings>Network>IP Network>H.323 Settings>New Password>[unique authentication password in double quotes, eg "Pa55w0rd"] Admin Settings>Network>IP Network>H.323 Settings>Confirm Password>[eg "Pa55w0rd"] Click the Update button at the top of the web page.
System Contact	Optional	Adding a system contact allows for easy identification of who is responsible for a VC unit. This contact could be responsible for co-ordinating bookings of the unit and/or for local troubleshooting should a fault occur.	From the unit's web interface select the following options: Admin Settings>Global Services>My Information>Contact Person>[Contact Name] Admin Settings>Global Services>My Information>Contact Number>[Contact Telephone] Admin Settings>Global Services>My Information>Tech Support>[Contact Name - Telephone Number if different] Click the Update button at the top of the web page.
System Location	Recommended	Setting a system location in the correct format will allows it to be included in the online directory mapping application being developed for SHOW.	From the unit's web interface select the following options: Admin Settings>Global Services>SNMP>Location Name>[xx.xxxxxx yy.yyyyyy nnnnn] Click the Update button at the top of the web page. Where xx.xxxxxx is the latitude, yy.yyyyyy is the longitude and nnnnn is the area code for the unit's ISDN lines or gateway, as appropriate, each field must be the correct number of characters long and separated by a single space character eg: Location Name> 57.123456 -4.123456 01234

Feature	Status	Reasoning	Instructions
Room Password	Recommended	Setting a Room Password prevents end-users altering settings on the endpoint.	The admin/room password is set by default with the machine's serial number. To change it: From the unit's web interface select the following options: Admin Settings>Security>Security Settings>Change Password.>Room[tick] Then Enter boxes. Click the Update button at the top of the web page.
Web Snapshot	Optional – depending on outcome of auto answer risk assessment. Systems assessed to have auto answer off should have web snapshots off.	With Web Snapshot enabled it is possible to view the unit's current video source via the unit's web page, thus allowing enhanced diagnostics if users are reporting issues with video.	For security reasons this change must be made locally to the unit using the remote control by: Call up the 'Home Screen' on the unit Select 'System' Select 'Admin Settings' Enter a 'Menu Password' if required Select 'General Settings' Select 'Security' Select 'Security Settings' Select the third page using the arrows at the bottom of the screen Tick 'Allow Video Display on Web'
Power button Function	Recommended	Ensures the power button on the remote puts the system to sleep or wakes it up rather than turning the system completely off thus rendering it unreachable.	From the unit's web interface select the following options: Admin Settings>General Settings>System Settings> Remote Control/Keypad> Power Button Function>[Sleep or Wake] Click Update at the top of the web page.

Feature	Status	Reasoning	Instructions
Home screen settings	Recommended	Leaves the Home screen with options to dial through the system Directory, or Place A Call manually, prominently placed. Ensures a user does not inadvertently dial the last number dialled by mistake. Also shows information to identify the unit correctly if requesting assistance.	From the unit's web interface select the following options: Admin Settings>General Settings>Home Screen Settings>Button 1>[Directory] Admin Settings>General Settings>Home Screen Settings>Button 2>[Place a Call] **Buttons 3, 4, 5 and 6>[None]** Admin Settings>General Settings>Home Screen Settings> System Name>[tick] Admin Settings>General Settings>Home Screen Settings>System[tick] Admin Settings>General Settings>Home Screen Settings>My Extension[tick] **Other tick boxes>[blank]** Click the Update button at the top of the web page.
Directory Servers	Recommended	By default a Polycom unit displays a directory/phone book called 'Polycom GDS' regardless of the actual name of the directory set on the unit. This name should be changed to reflect the directory set on the unit. Please note Polycom systems, at present, list one flat file directory so adding multiple directories to the unit often ends up with duplicate directory entries.	From the unit's web interface select the following options: Admin Settings>Global Services>Directory Servers> Polycom GDS>[tick] Admin Settings>Global Services>Directory Servers> Polycom GDS>Global Directory (GDS)[fill in appropriately e.g. the IP address of the TMS] AND [tick] Register. Admin Settings>Global Services>Directory Servers> Polycom GDS> Display Global Addresses>[tick] Admin Settings>Global Services>Directory Servers> Polycom GDS> Display Name in Global Directory>[tick] Admin Settings>Global Services>Directory Servers> Polycom GDS>Group Name>[fill in appropriately] Once done remember to click update at the top of the page.

13. Annex 4 – Endpoint Risk Assessment

System Name:_____ Location:_____ Date:_____

Risk	Possible Mitigations	Likelihood	Impact	Risk evaluation
Eavesdropping – user may be unaware that system is connected. Inadvertent release of sensitive or patient identifiable information.	Mic Off if using auto answer			
Inappropriate / malicious calls – senior staff members may be the target of inappropriate calls / interruptions / snooping.	Auto answer off Disable snapshots			
Sensitive location – system may be located in an area used by patients. Possible release of patient images.	Appropriate signage, Staff training Auto answer off Disable snapshots			
Very sensitive location – system located in an areas used for patient physical examinations. Possible release of intimate patient images.	Auto answer off Disable snapshots			
Home based systems – invasion of privacy.	Auto answer off Disable snapshots			