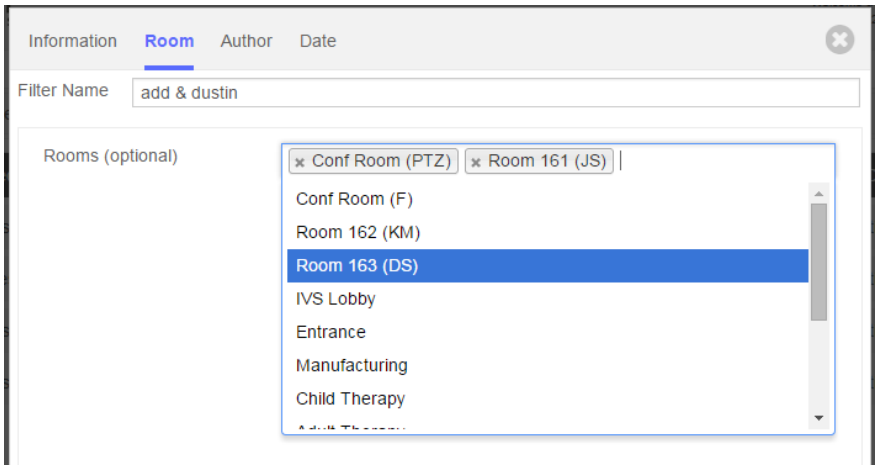
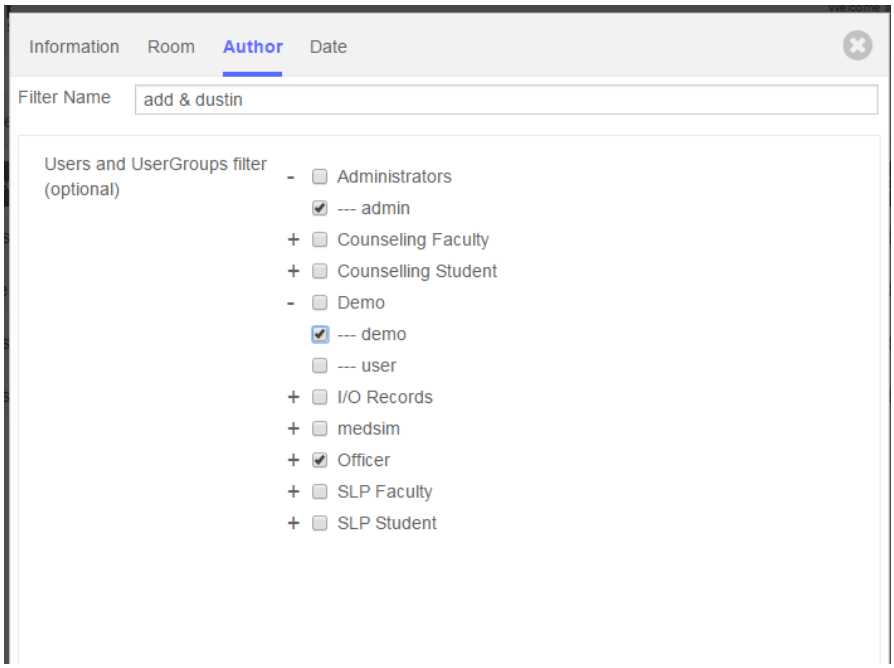
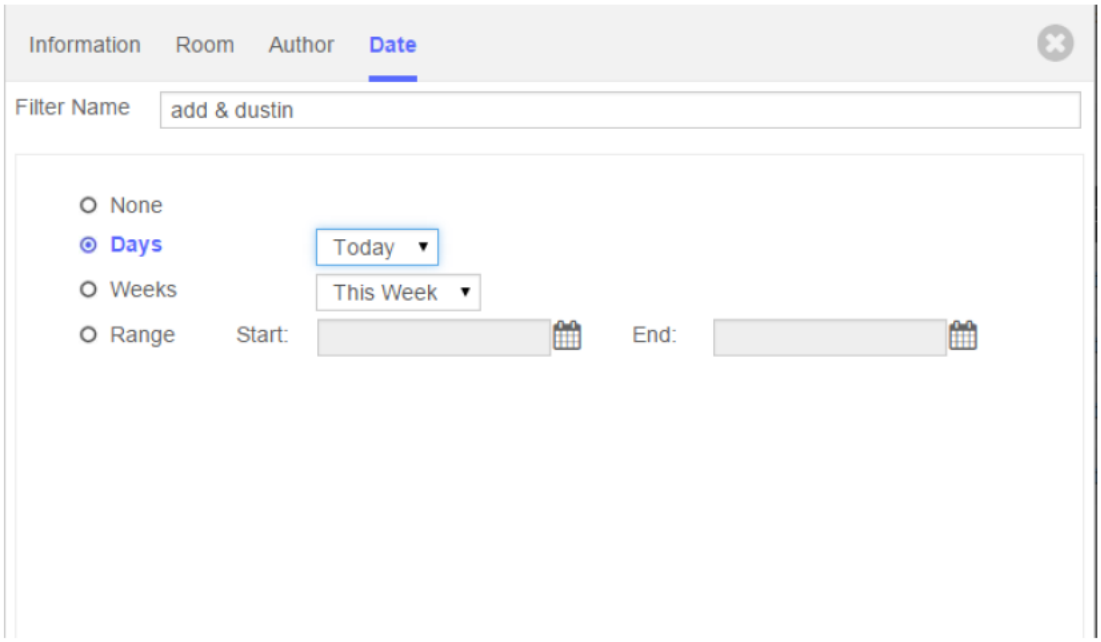
b) To filter on a specific room(s) click on the room section as shown below. Choose what rooms you would like to include, leaving this blank will display all rooms the active user has access to when the filter is applied.



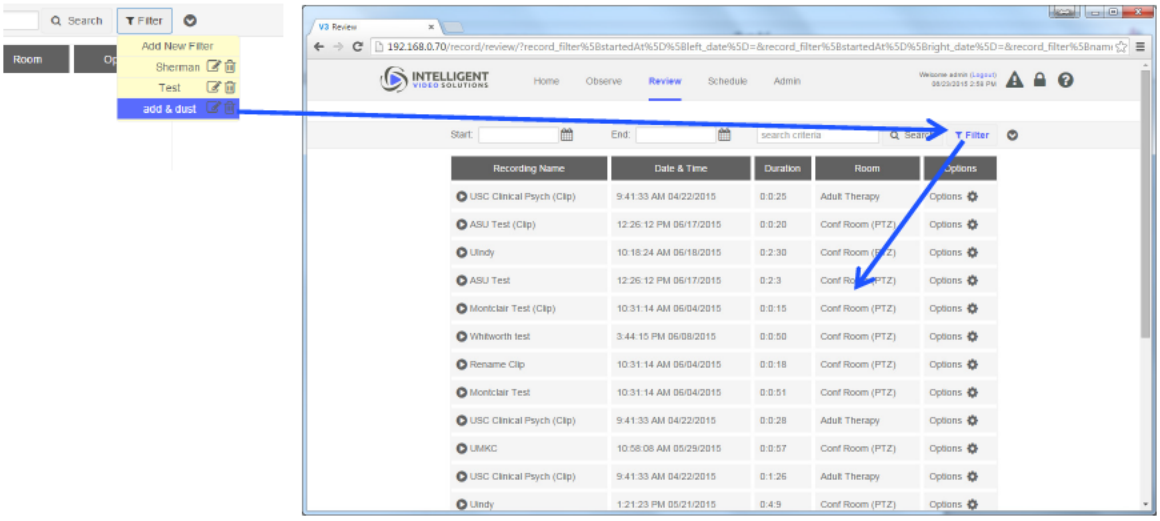
c) To filter on an author click on the author section. Leaving this section blank will display all authors active user has access to when filter is applied. To filter by a specific author or user group check the appropriate box(es) under this section as shown below.



d) To filter on a date or date period / range you can select the date section. Using the date section users can filter started today forward or back a number of days or weeks. Users can also set a static date range.

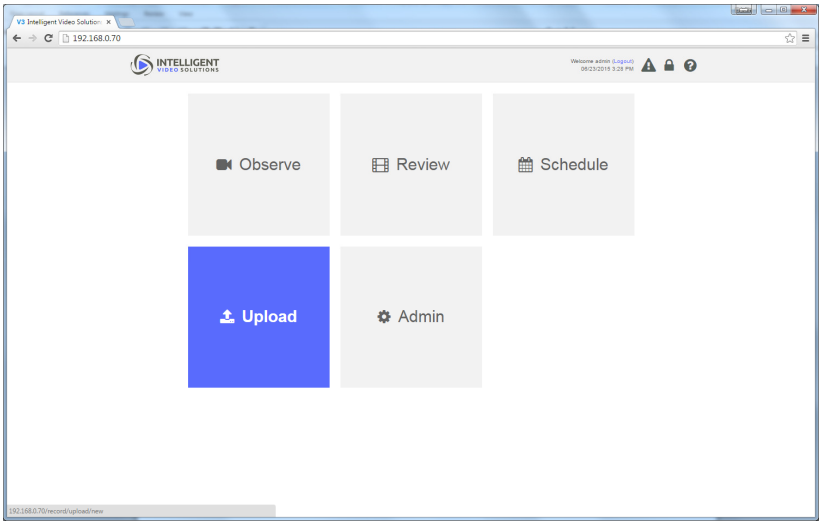


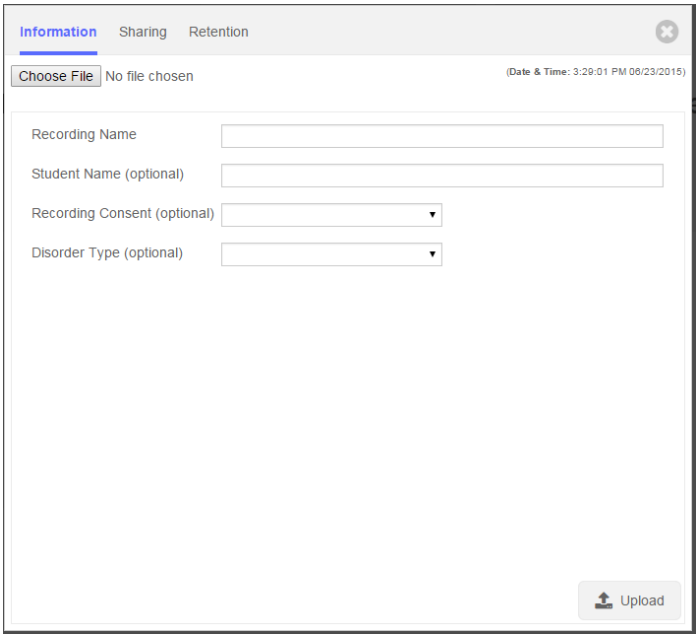
e) When the user is done setting up the filter sections make sure the filter has a name then click the save button. This filter will show up under the filter button when it is pressed for this user when in both the review and schedule sections of the application. To apply the filter select it as shown below. When the filter is active corresponding results will show and the filter button will appear blue (enabled). To disable the filter simply click the filter button a second time.



Upload

1) Overview: The upload function allows users to add video recorded using 3rd party devices to the system for security and management purposes. The video must be in a .mp4 format to be uploaded.
2) Uploading a video: To upload a video click on the upload icon under the home section as shown below:





a) Select the file to upload then enter the associated information, next set the sharing permissions using the sharing section and the retention period. Click upload to add the video file to the Valt database.

N66W38493 North Woodlake Circle, Oconomowoc, WI 53066
richard@cvisecurity.com PH: 262-569-1986 www.cvisecuritysolutions.com

RADFORD UNIVERSITY

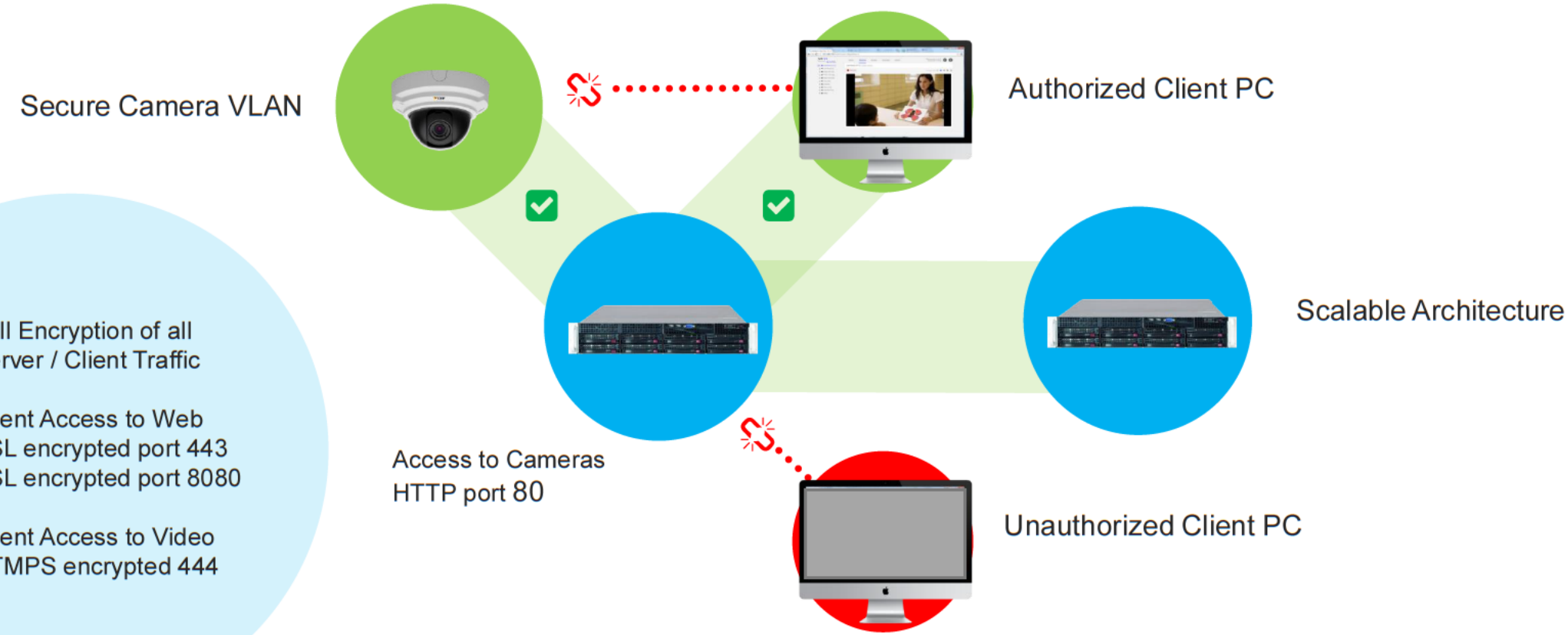
DEPARTMENT OF PSYCHOLOGY

CLINIC OBSERVATION RECORDING SYSTEM

GROUP ACCESS ASSIGNABLE RIGHTS

Functional Description	Admin-istrator	Faculty	Graduate Student	Under-Graduate Student	Visitor	Description of Allowance:
Observe:						**Allows users to access the observe section and do live observation on the rooms they have access to.**
Talkback: if enabled						Allows users the ability to talk back through the camera into the room if talkback hardware is in place. (Admin, Faculty),
PTZ Control: if enabled						Allows users to move PTZ cameras associated with the rooms they have access to as long as another user does not have an active session recording on that room
Edit Presets: on PTZ						Allows users to delete and create preset positions on the cameras associated with rooms they have access to.
Can PTZ all authors:						Allows users to move PTZ cameras associated with rooms they have access to regardless of whether or not another user has an active recording in progress for that room.
Review:						**Allows users access to the review section and perform searches.**
Add / Edit Markers and Info						Allows users to add markers during playback. Markers are points of interest within the recording.
Remove Markers						Allows users to remove markers during playback.
Playback Tools						Gives users' access to jog shuttle control and full screen buttons during playback.
Delete Recordings:						Allows users to delete recordings that show up within their search results.
Download Recordings:						Allows users to download recordings that show up within their search results.
Edit Information:						Allows users to edit the searchable information associated with recordings that show up in their search results.
Sharing:						Allows users to grant other users that normally would not have access to the selected recording, that recording will then show up in the specified users' search results
Retention:						**Allows users the ability to change the default retention period for the selected recording**
Schedule:						Allows users to schedule recorded sessions.
Add Schedules:						Allows users the ability to add new scheduled recordings
Exceptions:						Allows users to create exception dates. Exception dates are days where all scheduled recording functionality is suspended
Edit Schedules:						Allows users the ability to go back and edit scheduled start, stop time, searchable information, and any other rights they have below (example: sharing, retention etc.)
Delete / Remove Schedules:						Allows users to delete the next instance of a recurring schedule or remove a schedule completely
Sharing:						Allows users to grant other users that normally would not have access to all videos a schedule produces to that schedule, those videos will then show up in those users search results.
Retention:						Allows users the ability to change the default retention period for all recordings the selected schedule will create
Control:						**Allows users the ability to automatically move any PTZ cameras to a predefined position at the beginning of a scheduled recording**
Instant Recording:						Allows users to initiate a recording on the selected room when in the observe section
Stop all authors:						Allows a user to stop a recording regardless of who started the recording. By default users are only able to stop recordings that they have started.
Sharing:						Allows users to grant other users that normally would not have access to all videos a schedule produces to that schedule, those videos will then show up in those users search results
Retention:						Allows users the ability to change the default retention period for all recordings the selected schedule will create
Add Markers/Annotations:						**Allows users to add markers/annotations during live observation.**
UpLoad:						Allows Users to upload external MP4 recordings
Alert:						
Admin:						**Gives users access to the admin section.**
General:						
Templates:						Allows users to add / remove information and marker templates.
Rooms:						Allows users to add / remove / edit rooms and cameras.
Users & Groups:						Allows users to add / remove / edit users and groups.
Logs:						Allows users to view the systems audit trail and logs.
Help:						Allows users to modify the text associated with the help link that shows up for all users in the upper right hand corner.
Wowza						

NETWORK ARCHITECTURE: SECURITY & ENCRYPTION



- Full Encryption of all Server / Client Traffic
- Client Access to Web
  SSL encrypted port 443
  SSL encrypted port 8080
- Client Access to Video
  RTMPS encrypted 444

PRESENTS

INTELLIGENT VIDEO SOLUTIONS

VALT Software Specifications

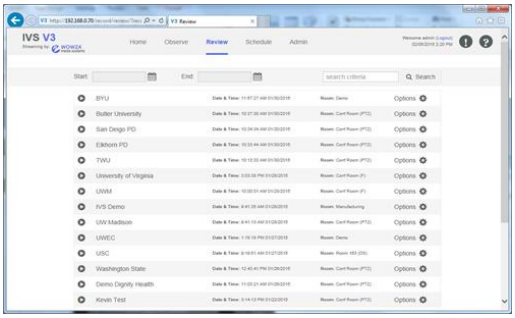
SUPPORTED IP CAMERAS
- All Axis P and Q Series Cameras
- Panasonic iPro Cameras

SUPPORTED IP ENCODERS
- Axis Q7401 Encoder
- VS-102-HDI HDMI Encoder

HARDWARE REQUIREMENTS
- Max 25 Cameras on Single Processor Xeon
- Max 50 Cameras on Dual Processor Xeon
- Runs on Ubuntu Server 14.04 TLS

USER PERMISSION FEATURES
- Observe Access per Room
- Talkback
- PTZ Control
- Review Access per Recording
- Add / Edit Markers
- Delete Recordings
- Download Recordings
- Edit Search Information
- Sharing
- Edit Retention of Recordings
- Add Scheduled Recordings
- Administration
- Add / Edit Rooms & Cameras
- Add / Edit Templates
- User Logs
- Edit Help Information
- Add Edit / Users & Groups

CAMERA CONTROL FEATURES
- View Live Video and Audio per Room
- View up to 9 Cameras Simultaneously
- PTZ Control on Supported Cameras
- Digital PTZ on all Cameras, Live and Recorded



CUSTOMIZABLE SEARCHABLE INFORMATION
- Customizable Fields per User Group
- Fields can be Drop Down, Text, or Static Text
- Fields can be Required

SEARCH FEATURES
- Recordings are Searchable by Information
- Author
- Date Range

SUPPORTED BROWSERS
- Chrome
- Firefox
- Internet Explorer
- Safari
- Puffin (Mobile)
- Dolphin (Mobile)

SOFTWARE FEATURES
- Intuitive Easy to Use Interface
- Full Motion Synchronized Audio / Video
- Full Featured Scheduler
- Bookmarking (Markers)
- SSL Integration
- LDAP Integration
- Digital Zoom Both Live and During Review
- Supports up to 4 Cameras per Room
- Cross Platform Support (PC, MAC, Tablet)

Initiate recordings on demand or schedule them in advance.
Easily find recorded video using our built in search interface.

R16-024
11/20/2015 Negotiation Meeting w MCW to include IVS upgrade demo

RU: Jeff Aspelmeier, Ed Oakes, Randy McCallister, Jennifer Mabry, Kevin McDowell; Stephen Owen (out of town).

Topic: MCW, CVi, and Intelligent Video Solutions (IVS) will demo the updated CVi CORS solution now proposed.

Ed – partnership between IVS and CVi and MCW – who is doing what
Vendor - CVi reseller of IVs. IVs developer, sells to system integrators like CVi. CVi takes system and matches with servers, cameras and all equipment. Sofware & server supported by IVS – get hardware warranty and all service. Camera/audio supported by MCW.

Nancy – Chase will email Nancy the PowerPoint presentation.
Vendor – Rebeccca just upgraded software to this CORS, but may not have implemented all functionality.

Original market was police interview. With advent of IP cameras they modified to second generation ISR. That's what RU used for speech therapy. Now third gen is VALT. Much as we're seeking. Multiple servers shared among multiple depts.. Supports max 50 cameras per server – dual processor server, 1mp cameras, 750p.

Purpose built application to observe live vid/aud and record same. Almost exclusively in Higher Ed clinical environment. Hippa compliant. Can also do nursing, pharmacy simulation. Also students working w live patients in clinic.

Axis camera line almost exclusively – most validation. May work with other camers. Dome cameras can mount on ceiling or wall. Most clinical use wall mount since ppl seated – model 3364. Mount on wall about 60-65" on wall, as low as 3' off ground for children. Ceiling mount more in medical, wall mount more in clinical. Wll 5414 and 5415.

Have privacy switch to disable audio/video access – contols up to 2 cameras from single switch – m/b specified. Kills network connection. Assembled at IVs, kills network, not power to camera. Small lag for camera to reconnect to network. No power delay. Can customize to kill 4 cameras in one room if we request.

Server 2U R8x10D good for our needs.

Server software Ubuntu.

Software demo –

Server(s) on our network. Can be exposed to Internet or not, usually not. Client, from any networked computer can access server cluster if authorized. Can cluster all servers together so it seems to be one access point for end user.

>>> Can email me a video for reference

Everything can be enabled or disables (hidden) depending on user rights. Demo is admin – full access.

Drag and drop rooms/cameras into pane – single, quad, 3x3. Default audio is upper left, click to switch to another room. If multi-cameras in one room, audio is recorded with each camers identically. Only plays the active video's audio to avoid echo. Provides redundancy. Can pan, zoon. Can define presets naming unique points in the room – presets. Good for recording sessions, alsways starts at the preset location.
Talkback – usb microphone or headshet allows talkback into room into wireless body pack and earbu or speaker. Signal goes into monitoring computer to earbud. Server sends audio back through camera – audio in and out. Audio out links to earbud/body pack – no extra cabling. Wireless transmitter.

Handheld and digital zoom. What you see all viewer see, except digital zoom doesn'timpact what others see or video records. Fixed cmeras can alsozoom – digital zoom. Can click and drag to move, even on fixed camera.

Initiating recording – adhoc, select room, click record, complete info template fields to identify recording. Then easy to search. Customizable by users, typically limited to subset to users – perhaps sr faculty or clinical directors. Access through web portal. Can have blank fields or drop-down menus. Can even save audio note. Other tabs beyond info – sharing, retention. Deifines who has access to video based on whos recording. Can check video access users – category, indiv, position. Usually set up so students can only see their videos. Retention – define how long to keep recording before deleting – keep until ___ or set ___ days, etc. If don't' have access to view, also can't hear.

When press "stop" button and view/record instantly stops. Can imbed marker into video to provide feedback and notes. Allows viewers to jump back to marked points. Can enter feedback in playback as well. Can have lit led indicator and can combine w/ view/record kill switch.

Schedule feature – set up roms and all info in advance. Segment videos to control access – multiple methods. Control tab to preset camera location. Can search recorded videos by date range, advanced search by disorder type or student name and/or more as filters. Find red markers on videos easily. Add and search for markers.

Editor tool can clip section out of longer video – cue in and cue out, create clip between ticks you entered. Keeps same security controls and recording anem/ disorder, ets as original. Suport up to 9 cameras in a single room,

Ed – best number cameras per size, PTZ vs fixed.
Vendor – treatment room, small, two or less cameras. Group therapy up to 4 camers, usually min 2. Med sim may have 4 or up in med simulation suite. Higher pixel helps with clear zoom. If use PTZ more often have one PTZ and one fixed in same room.

Record start/stop and kill switch can be customized to be on one switch. Latest quote included this. We want kill switch disconnects network, but on/off only controls recording, not viewing/listening.

Recorded video – w/ access can change video info, can download, can export w/o render or conversion process. Can be used on pdf or other. Can integrate with w/ ipad and ios devices allows phone/pad to turn into mobile camera. T's a floating camera linking into system. Can eve go offisite, record, come back onsite and sync into system. If not in streaming need to lon into system. If offsite, stores locally on ipad. Put on kiosk mode to lock down – record to ipad and when in range will upload to server. Using ios device is not HIPPA compliant unless locked down and can't connect to other networks.

Not really focused on admin section. Audit trail – keeps detailed trail, who logged in from what computer, who start/stop/review/etc.

Ed – limit on number of logged in users. Hardware limit on network stream. Server 2gig nics.
Ed – authentication. Use local users/groups set up in admin panel. Can have LDAP tie in, pair inside software. Can manually link using spreadsheet. Larger deployments use LDAP. Ed – we won't use LDAP in CAPS, but yes in rest of usage. V – can use mixed authentication.

Alert if running low in storage, also visible in logs.
If go w/ 2mpx cameras, 25-35 cameras w/ 1080p instead of 780p. 1.7xstorage limit.
Does RU want to use for docs or just ppl.
Jennifer – in playback – diff btwn fixed camera zoom vs. pantilt – different? No benefit to pantilt on playback unless already positioned in advance to specific point .

Typically 720p. Lg rooms 1080p model.

Ed – higher quality, fewer count saves us money.
V – can set 1080p camera can be set to 720p or 1080p – flexible.
V – if digitally zoom on fixed, does not impact record. On PTZ would limit record to what's zoomed.
Jennifer – CAPS may prefer fixed. Jeff – in rsch PTZ gives more flexibility. May be good to have both types in rooms. Esp larger rooms or child activities on floor. Jennifer – ipad can

RU only - Follow=up discussion after vendor mtg.
Cost for ipad license.
Randy - Clarify = existing software – can we receive upgrades through potential new contract?

SECURITY QUESTIONS FOR TECHNOLOGY-BASED PROCUREMENTS

Name of Technology	VALT Software
Name of Company	Intelligent Video Solutions & MCW Solutions, LLC.
Contact Information	Dustin Stern, 262.746.9292, dstern@ipivs.com Chase V. Fisher, 540-454-9318, CFisher@MCWSolutions.net

If purchased, the University reserves the right to conduct an IT security assessment on the product(s), system(s) and/or service(s) once delivered to validate the responses to questions below. If evaluation copies or instances are available for testing, they should be
provided to the IT Security Office through the Contract & Procurement Office prior to purchase.

1	**DOCUMENTATION**		
	Question	*Response*	*Internal Use*
1.1	Do you have a completed Shared Assessments full SIG questionnaire?	Not Applicable	
1.2	Have you undergone a SAS 70 or SSAE 16 audit?	Not Applicable	
1.3	Do you have a documented change management process?	Not Applicable	
1.4	Do you have a formal Incident Response plan?	Not Applicable	
2	**APPLICATION/SERVICE/DATA SECURITY**		
	Question	*Response*	*Internal Use*
2.1	Describe the level to which the roles and permissions can be customized by The University.	5 sections (Observe,Record,Review,Schedule,Admin) multiple permissions within each section. Application allows for complete customization including what videos users have access to for both live and recorded sessions. http://ipivs.com/wiki/Adding_a_User_Group	
2.2	What specific encryption algorithms are employed for your product(s), system(s) and/or service(s)?	Our system leverages apache and SSL for data encryption and RTMPS for video encryption. Both methods will utilize university provided certs AES-256 being the most common.	
2.3	Is all sensitive data (i.e. Social Security Numbers, Credit Card Numbers, Health Information, etc.) encrypted in transit and at rest? If not, please explain.	Transit via SSL rest option via full disk encryption.	
2.4	Will University data be encrypted at rest? (Whole Disk Encryption, DB encryption, column level encryption inside a DB)	Optional whole disk encryption typically not implemented.	
2.5	Describe the mechanism for transferring data from The University to your organization. Are these transfers logged?	NA	
2.6	Is login information such as user name and password encrypted during transmission from the client to the server? NOTE: Base-64 encoding is not acceptable.	Yes SSL	

2.7	Are passwords hashed, so they cannot be decrypted? (SHA-1, SHA-256, MD5, …)	Yes SHA-256	
2.8	Does your product(s), system(s) and/or service(s) prevent the use of shared credentials or accounts including administrative accounts?	Can be deployed however you choose. Typically each account will have unique creds.	
2.9	Describe how your product(s), system(s) and/or service(s) authenticate and authorize users?	LDAP, LDAPS, or local accounts all tied to local user groups.	
2.10	Does your product(s) and/or system(s) facilitate compliance with Federal and State laws, such as FERPA, HIPPA and PCI?	Yes.	
2.11	Is all access, including administrative accounts, controlled and logged (i.e. firewalls, file system permissions, ACLs, database table permissions, packet logs, etc.)? If not, please explain.	Yes, database tables.	
2.12	Will The University data be used in test or development environments?	NA (no)	
2.13	Does your company own the physical data center where The University's data will reside?	NA (system is not cloud based and will reside in Radford data center)	
2.14	Do any of your servers reside in a co-located data center?	NA	
2.15	If you are using a co-located data center, does this data center operate outside of the United States?	NA	
2.16	If this co-located data center operates outside of the United States, will any of The University's data ever leave the United States?	NA	
2.17	If The University data will leave the United States, please list all countries where it will be stored.	NA	
2.18	Is there a contract in place to prevent data from leaving the United States?	NA	
2.19	If you are using a co-located data center, please describe how networks and systems are separated.	NA	
2.20	Are intrusion detection technologies and firewalls utilized on the hosted system(s)?	NA	
2.21	Describe how your facility is physically secured?	NA	
3	**THIRD PARTIES**		
	Question	*Response*	*Internal Use*
3.1	Will The University data be shared with or hosted by any third parties?	Not Applicable	
3.2	If so, list all 3rd parties that will host or have access to The University data.	Not Applicable	
3.3	Do you perform security assessments of third party	Not Applicable	

	companies?		
3.4	If you do assess third parties, please describe assessment methodology.	Not Applicable	
3.5	How often do you reassess third party companies?	Not Applicable	
3.6	Briefly explain why each of these third parties will have access to The University data.	Not Applicable	
4	**PASSWORD/PASSPHRASE MANAGEMENT**		
	Question	*Response*	*Internal Use*
4.1	Can you enforce password / passphrase aging requirements?	Yes – University is control	
4.2	Can you enforce password / passphrase complexity requirements?	No – LDAP integration optional	
4.3	Are user account passwords / passphrase visible in administration modules?	No	
4.4	Are stored user account passwords / passphrases hashed?	Yes	
4.5	What algorithm is used to hash passwords?	SH-256	
5	**VULNERABILITY ASSESSMENT/MITIGATION**		
	Question	*Response*	*Internal Use*
5.1	The OWASP 10 identifies the most critical web application security flaws. How does your organization address and mitigate the common application risk identified by the OWASP Top 10. Information about the OWASP Top Ten can be found at https://www.owasp.org/index.php/OWASP_Top_Ten_Project.	Not Applicable	
5.2	Are your applications scanned for vulnerabilities by a qualified 3rd party?	Optional – they have been by other universities during audit processes	
5.3	Are your systems scanned for vulnerabilities by a qualified 3rd party?	Optional – they have been by other universities during audit processes	
5.4	Are your applications scanned for vulnerabilities prior to new releases?	Optional – they have been by other universities during audit processes	
5.5	What application and operating system vulnerability scanning companies do you use?	Not Applicable	
5.6	How often are operating systems and applications scanned?	Not Applicable	
5.7	Are updates to your product released on a regular schedule?	Yes at minimum once a quarter	
5.8	How are critical security patches applied to your systems and applications?	Can be set for automatic or scheduled up to the University	
5.9	Will we be notified of major changes to your environment that	Not Applicable	

	could impact our security posture?		
5.10	Computer and network security is of paramount concern. The SANS Institute and the FBI have released a document describing the Top 20 Internet Threats. How does your organization address and mitigate the common application risk identified within the Top 20 Internet Threats? The document is available at www.sans.org/top20.htm for review.	Not Applicable	
6	**DISASTER RECOVERY/BACKUPS**		
	Question	*Response*	*Internal Use*
6.1	Do you have a disaster recovery plan?	Per Addenda 2 Q&A #3, Not Applicable.	
6.2	Are components of your disaster recovery plan located outside of the United States?	Per Addenda 2 Q&A #3, Not Applicable.	
6.3	When was the last time you tested your disaster recovery plan?	Per Addenda 2 Q&A #3, Not Applicable.	
6.4	Are you performing backups?	Per Addenda 2 Q&A #3, Not Applicable.	
6.5	What type of media is used for backups?	Per Addenda 2 Q&A #3, Not Applicable.	
6.6	How long are these backups kept?	Per Addenda 2 Q&A #3, Not Applicable.	
6.7	How is backup media destroyed?	Per Addenda 2 Q&A #3, Not Applicable.	
6.8	Are you encrypting your backups?	Per Addenda 2 Q&A #3, Not Applicable.	
6.9	Will you be willing to encrypt backups of The University data?	Per Addenda 2 Q&A #3, Not Applicable.	
6.10	Are these backups taken offsite?	Per Addenda 2 Q&A #3, Not Applicable.	
6.11	Where are all the locations that will store The University backup data? Please list by country if located outside of the United States.	Per Addenda 2 Q&A #3, Not Applicable.	
7	**EMPLOYEE POLICIES/SECURITY AWARENESS**		
	Question	*Response*	*Internal Use*
7.1	Do you perform background screenings on employees?	Yes. MCW is a Department of Defense Industry Contractor (Cage Code 3FBG8-I), and all employees are subject to investigations to the Secret level.	
7.2	Do you have an information security awareness program?	Yes, per the response of section 7.1, all employees undergo initial and annual protective measures and awareness refreshers.	
7.3	Is the security awareness training mandatory for all employees?	Yes, for all essential and cleared personnel, which makes up about 90% of the company. Our Facility Security Officer, Chase V. Fisher, can be reached at CFisher@MCWSolutions.net or 540-454-9318	
7.4	How frequently are employees required to undergo the security awareness training?	Annually.	

7.5	Do your employees hold Information Technology Security certifications and/or secure coding? If so, which ones?	Microsoft, Cisco, Dell. CCNA, MCSE, CCPS, CQS-FSPS, CQS-CCENT, CQS-CSSSER, CSE,CSE 6.0, CCPS1 and many more.	