Orlando VA Health Care System (OVAHCS)

Physical Security, Electronic Security Systems, Locks and Keys Specifications

This document supersedes any conflicting guidance or contractual terms in contracts including leases.

The authority holding jurisdiction (AHJ) for physical security matters for the United States Department of Veterans Affairs (VA) Veterans Health Administration (VHA) is the Assistant Under Secretary for Health for Support Services or their delegate the Healthcare Engineering Oversight Committee on Physical Security and Resiliency. VA Police Physical Security is the Subject Matter Expert in Physical Security Matters. Should there be an impasse due to conflicts in interpretation between any party and VA Police Physical Security, VA Police Physical Securities interpretation shall be used unless a memo by the AHJ is approved and sent to VA Police Physical Security. Contact Orlando VA Police Physical Security for the most current specifications and interpretations, this is a living document that will frequently change. All sites, including leases, must abide by VA Handbook 0730, VA Technology Reference Model (https://trm.oit.va.gov/TRMHomePage.aspx) and VA Physical Security and Resiliency Design Manual (PSRDM). Leased sites may abide by the Cybersecurity & Infrastructure Security Agency (CISA), Interagency Security Committee (ISC), Facility Security Level (FSL) determination requirements in accordance with the PSRDM or abide by the PSRDM requirements. The PRDM and 0730 may be found in the VA Office of Construction & Facilities Management Technical Information Library (CFM TIL) found at https://www.cfm.va.gov/til/ . The PSRDM Appendix B "Security System Application Matrix" describes the minimum locations for electronic security systems. The FSL shall be determined by the VA Police Physical Security as they are the only entity within the VA with access to the evaluation tool. Items not addressed in the FSL requirements shall abide by the PSRDM and the PSRDM appendices or be guided by VA Police Physical Security. Any conflicts between these requirements and contracts shall be settled by VA Police Physical Security or the AHJ. All proposed physical security, electronic security systems, locks and keys shall be presented to the Physical Security Specialist or Police Service delegated person for approval and a list of proposed components shall be provided. All electronic security systems shall integrate into a "single pane of glass" (all Electronic Security Systems such as but not limited to cameras, intrusion, key management, etc… shall be integrated into the access control system where and when possible) as per the PSRDM, currently this is LenelS2 OnGuard 8.1. Any deviations from the specified systems below shall require written approval from the OVAHCS Physical Security team. The VA locksmith shall be consulted for all locks and keying. Please refer to the PSRDM and VA Handbook 0730 for the minimum required electronic security system components. All equipment must be TAA and NDAA compliant. Equipment should be on the GSA Advantage site to avoid additional vetting requirements. VA Police Physical Security may be contacted at vhaorlpolicephyssecurity@va.gov.

Surveillance Camera Systems:

1) Lake Nona is the head end and runs Pelco VideoXpert Enterprise
2) Other than Lake Nona:

a. Locations that are not expected to go over 100 cameras: VideoXpert Pro and all required components and licenses to allow integration into the Lake Nona Enterprise (Head End) system.
    i. Pro servers shall be “Power” series running Windows Server 2019 or better with a RAID 6 storage configuration.
    ii. Contact Physical Security to determine what licenses if any are needed for expansions.
    iii. New locations shall support a minimum 10% growth.
b. Locations with over 90 cameras (within 10% of the 100 camera recommendation) shall use a VideoXpert Enterprise setup all required components and licenses to allow integration into the Lake Nona Enterprise system.
    i. Each Enterprise site shall have a CMG (CMG/CMG2/CMG3/etc…) and appropriate storage for the number of cameras on site.
    ii. Each Enterprise site shall have a redundant CMG and fallback storage server.
        1. The redundant CMG shall be a second CMG of the same or better model as the primary.
        2. The fallback storage server shall be of sufficient size to store 15 days of video should the largest size storage server on site fail.
    iii. Each Enterprise site (other than Lake Nona) shall have sufficient Enterprise Aggregation Licenses added to the Lake Nona head end to aggregate the system.
    iv. Each Pro site shall have sufficient Pro Aggregation licenses added to the Lake Nona head end to aggregate the system.
    v. New locations shall support a minimum 10% growth.
    vi. Existing locations that reach 90 cameras shall be evaluated by Physical Security to determine if migration to an Enterprise system is needed.
c. Storage servers shall be:
    i. Checked to ensure they are set to RAID 6 with the formatting to allow the maximum expansion capability for that server.
    ii. Checked to confirm the storage array is set as the recording pool
    iii. Checked to confirm the OS drive is not in the recording pool

3) We are currently running VideoXpert 3.21 (Enterprise and Pro) and are migrating to 3.23 (last update 02-15-2024) .

4) Cameras:
a. When adding cameras or upgrading existing cameras the vendor must confirm the required storage is available and include additional storage when needed.
    i. Storage capacity must allow for a minimum of 30 days 24/7 recording
    ii. Storage shall be based on the camera’s maximum resolution settings
    iii. Storage shall be based on recording at 30 fps
    iv. Smart compression should be set to low
    v. Storage shall have an additional 10% buffer to the above.
    vi. Storage servers shall be E288 (288TB) or larger.
b. Cameras shall be powered via PoE unless approved by the COR/Program Manager.
    i. PoE injectors may need to be provided for cameras requiring over 30 watts of power. Check with the COR/Program manager to confirm switch port PoE rating.
    ii. Media converters may be used when distances are greater than the distances certified for ethernet Cat6a cabling.

iii. Media converters shall have Uninterruptable Power Supplies (UPS) supplying the camera end to ensure operation until generator power is established during outages.

c. Pelco/Avigilon is the preferred camera manufacturer (CUSTOMER NAME: Orlando VA Medical Center. CUSTOMER ACCOUNT # 3134353 must be given to Pelco for estimates and orders). Cameras shall be the better of Pelco professional or enterprise-grade cameras and be submitted for approval to Physical Security. Other manufacturers' cameras may be submitted for approval and shall be equivalent or better of the closest Pelco equivalent.
d. All necessary housings, adaptors, mounts and other accessories shall be provided by the contractor for camera additions and replacements.
e. Cameras housings in "Clean" areas (surgery, sterile storage, etc...) shall be of appropriate materials for the area and suitable for cleaning with chemicals used for sterile area cleaning. Harsh environment stainless steel housing preferred.
f. Must have "night mode" with infrared illuminators.
g. Must be capable of H.264 and H.265 recording.
h. 3MP resolution or better with a minimum 16:9 aspect ratio capability.
i. Multidirectional (180, 270 and 360 degree) cameras that "stitch" the views together are preferred. I.E. Pelco Optera series multiviews are preferred over the Sarix series due to their panoramic view and lower power requirements. Axis cameras are acceptable.
j. Axis multidirectional cameras with attached PTZ cameras are acceptable where appropriate.
k. Multi-lens cameras such as those with dual and triple independently aimed camera lens heads are acceptable where appropriate.
l. Installation of additional cameras shall include all required licensing. Support type licenses that require renewal shall be provided for a minimum of 3 years.
    i. Contact VA Police Physical Security with any questions and to confirm counts.
        1. Currently, Enterprise Channel Licenses are not needed for the Lake Nona system due to unused licenses in that system. Date: 10-03-2024.
        2. Enterprise channel licenses may be needed for other Enterprise systems.
        3. Pro channel licenses may be needed for Pro systems.
        4. 3 year SUP (Software Upgrade Program) licenses shall be provided for each additional camera installed.
        5. Aggregation licenses, Enterprise and Pro as applicable, shall be included based on the system the cameras are being added into.
        6. All required licensing to allow integration into the ePACS and associated Electronic Security Systems (ESS) shall be included. The OVAHCS Currently uses LenelS2 OnGuard 8.1 for its ePACS.
        7. Contact Physical Security to determine if any other licenses are needed.
m. Cameras shall be named in all web and Video Management System (VMS) interface fields.
    i. The naming convention shall be Facility, Building, Floor, Area, Room/Landmark IE: LN - Hospital 2nd floor Keyless/PIV office area 2K702C.
    ii. A check shall be done to confirm that the name shows in toolbox and ops center.
n. IPV6 shall be turned off.

o. Camera maps shall be created or updated and uploaded to the appropriate systems where needed.
p. Existing sites without maps shall have one created.
q. Camera locations shall be added/updated when new cameras are installed.
r. Cameras shall be approved by VA Police Physical Security and the VA Locksmith.

5) Cameras shall be configured to:
   a. ICS network Time Server
   b. 16:9 or better if capable
   c. Video Streams
      i. Primary stream shall be set to the maximum resolution 15fps
      ii. Secondary shall be one setting down 7.5fps
      iii. Tertiary shall be one setting down from secondary 5fps
      iv. Some cameras may be set to higher recording rates at the discretion of VA Police Physical Security
      v. Compression shall be set to low.
   d. Pan Tilt Zoom (PTZ) cameras shall have their "startup point" defined and set to a "useful" location. See item 11.
   e. PTZ cameras should be paired with "Multiview" cameras for full coverage where appropriate.
   f. Audio shall be disabled as a default. Specific cameras may be identified as needing audio enabled.
6) Must provide the greater of 1-year parts and labor warranty or manufacturer warranty with labor costs included for all systems to be maintained by the OVAHCS starting on the turnover date.
7) Must be installed and supported by a Pelco VideoXpert Enterprise Certified installer
8) A workstation shall be provided for local camera viewing at all new facilities.
   a. Multiple shared displays may be needed at new locations. Contact Physical Security for locations.
9) All computers/servers
   a. Including shared displays shall have "turn on after power loss" enabled in BIOS
   b. Configured for remote desktop connections.
   c. Turn off IPV6 in the network settings.
   d. Updated to the current VideoXpert version being used by the OVAHCS
   e. Once connected and after update, toolbox shall be checked to confirm the version shows correctly in Toolbox.
   f. Confirm all licenses have been applied and that Physical Security has added the license(s) to the licensing portal account.
   g. Confirm all firmware and drivers are up to date.
   h. All devices capable of having dual power supplies (such as networking devices and servers) shall include both power supplies.
10) Network interface cards (NIC) Teaming shall be set up for storage servers when they have more than one NIC. Contact the VA Locksmith for clarification and correct configuration.
11) Contractors working on the servers must be Pelco VideoXpert Enterprise certified and have the appropriate background check level.
12) Contact Physical Security for clarification.

Electronic Physical Access Control System (ePACS):

1) **Contact VA Police Physical Security to confirm the ePACS system to be installed.**
2) The Orlando VA HCS uses PIV 5.5, 7, and 8.1 cards. Currently, PIV 8.2 cards are approved but have not been deployed by the federal government. The ePACS systems shall be able to use all cards deployed by the federal government and be upgradeable for future PIV cards.
3) Contact Physical Security to determine what licenses if any are needed.
4) The Orlando VA Health Care System is transitioning all sites to LenelS2 OnGuard Professional 8.1:
    a. All systems will be connected to the "Head End" at Lake Nona.
    b. System will use GSA IDManagement.gov APL 10126. See FIPS 201 Approved Products List - Physical Access Control System Components (idmanagement.gov) for details.
    c. Power supplies and door controllers shall be life safety with batteries for redundant power.
    d. System Controllers: LenelS2 – LNL-X4420. (This is the only allowable controller for readers for a FICAM-compliant OnGuard system). 16 door readers max per LNL-X4420 to ensure future FICAM upgradability. 8 doors max if all require high security.
    e. Interface boards LenelS2- LNL-1300-S3, LNL-1320-S3, LNL-1324e and the LNL-1100-S3, LNL-1200-S3.
    f. LifeSafety Power power supplies
    g. Validation system software, components, and licenses (All purchased through LenelS2)
        i. TI EntryPoint EP—EWS base License
        ii. TI EntryPoint EP-PNL-RDR Panel/Server License, per controller, 2 readers
        iii. TI EntryPoint EP-ADD-RDR-2 Additional 2-reader license
        iv. TI EntryPoint EP-ADD-BWS Additional Enrollment Station
        v. LenelS2 SWG-AUTH-002 – OnGuard High Assurance reader, bundle of 2.
        vi. PIV Readers licenses (All purchased through LenelS2) LenelS2 Veridt 900W2036-QXYON Stealth Dual (Part number not yet verified for appropriate firmware version. Alternate part number may be required.)
    h. Card Readers shall be configured and flashed for Weigand. Card readers must be upgradable to OSDP:
        i. Veridt Dual Bio Contact/Contactless Reader (APL# 10092)
        ii. Veridt Stealth Dual Contact/Contactless Reader (APL# 10093)
        iii. Veridt Stealth Lite Dual Contact/Contactless Reader (APL# 10094)
        iv. Veridt Stealth Contactless Reader (APL# 10095)
        v. Veridt Stealth Lite Contactless Reader (APL# 10096)
        vi. Identiv uTrust TS Reader with Keypad (contact/contactless) (UTR-9216 XXXX-LNL) (APL #10153)
        vii. Identiv uTrust Contact TS Reader with Wallmount (contact/contactless) (UTR-9116- XXXX-LNL) (APL #10152)
        viii. Identiv uTrust Mullion Contactless Reader (UTR9002-XXXX-LNL) (APL
        ix. #10154)
        x. Identiv uTrust Wall mount Contactless Reader (UTR9102-XXXX-LNL) (APL #10155)
        xi. Identiv uTrust Wall mount Contact/Contactless Reader (UTR9106-XXXX-LNL) (APL #10156)

xii. Identiv uTrust Keypad Wall mount Contactless Reader (UTR9202-XXXX-LNL) (APL #10157)
xiii. Identiv uTrust Keypad Wall mount Contact / Contactless Reader (UTR9206-XXXX-LNL) (APL #10158)
xiv. Alternates may be submitted for approval to VA Police Physica Security and the locksmith.

i. The door access control communications protocol is currently Wiegand. This will be converted to OSDP in the future and the appropriate cabling shall be in place to allow for this.
j. Enclosure and contents must be UL certified as a complete unit.
k. Contact VA Police Physical Security if any clarification is needed.

5) Orlando VA HCS Legacy ePACS systems –
   a. LEGACY SYSTEMS – used where applicable, contact VA Police Physical Security:
      i. AMAG/Symmetry 8.0.2 Homeland Security Edition (Lake Nona) **Should be replaced by May 2025**
         1. Javelin S8 series card reader with PIV 5.5, 7, 8.1 and 8.2 compatible firmware.
         2. Contact VA Police Physical Security for panel information.
         3. Altronix power supplies
      ii. Identiv Hirsch hardware. (all other locations) **Should be replaced by May 2025 at Lake Baldwin, Lakemont and Viera.**
         1. Currently running Velocity 3.8.4
         2. Mx series control panel's.
         3. Altronix power supplies.
         4. Must use SNIB 3's for future FIPS compliance.
         5. Must include components for FICAM HSPD-12 compliance.
         6. Must use PIV Class card plus Pin pad reader that can read PIV 5.5, 7, 8.1 and 8.2 cards.
            a. Preferred Card Reader: Veridt 900W2036 using Weigand protocol with capability to be used with Lenel OnGuard.
            b. All others must be approved
            c. Potential alternate readers
               i. HID pivCLASS RPK40
               ii. HID pivCLASS RKCL40
               iii. HID pivCLASS Biometric Reader
               iv. HID Signo 20K PIV
               v. HID Signo 40K PIV
   b. **The Orlando VA HCS is transitioning to LenelS2 OnGuard v8.1. All ePACS installations (expansions of existing facilities and new facilities) expected to come online shall be LenelS2 OnGuard unless otherwise approved by VA Police Physical Security**.

6) Must include all required additional licensing where applicable. Contact Physical Security to determine what licenses if any are needed to include required integrations such as but not limited to:
   a. Key management
   b. Camera system
   c. Intrusion Detection
   d. Intercom

    e. Camera Analytics
    f. Visitor Management
7) All systems must be installed by installers certified by the appropriate manufacturer.
8) When installing new readers, the access control cabling must be OSDP compatible.
    a. May be composite cable such as ANSI: 4461030-500/OSDP 1 4 Elem Comp Cable CMP Ylw Jacket along with any additional cabling needed for FICAM compliance to include meeting manufacturers' recommendations for cabling or similar cabling meeting the manufacturer's requirements. We have been advised the minimum requirements for cable are:
        i. 1-22/24awg 2 twisted individually shielded pairs (TSP) for reader.
        ii. Longer distances may need dedicated power to the reader.
        iii. 1-18awg 4 conductor for rex.
        iv. 1-18/22awg 2 conductor for contact.
        v. 1-18awg 4 conductor for electric locking hardware.
        vi. Contact Physical Security if there are more than 4 end devices.
    b. Cabling distances may require larger gauge conductors to meet power requirements.
9) Greater of 1-year parts and labor warranty or manufacturer warranty with labor shall be included for systems to be maintained by the OVAHCS starting on the turnover date.
10) Contact Physical Security for location requirements.
11) On multidoor entrances, all exterior doors shall be on the electronic access control system.
12) Systems shall be managed by the VA.

Intercom Systems

1) OVAHCS is currently using AIPHONE IX series for its intercom solution with firmware v6.1.

Intrusion Detection Systems (IDS):

1) All VA managed IDS not integrated with the access control systems will be monitored by the Department of Homeland Security, Federal Protective Services, MegaCenter when the VA is responsible for the alarm. All equipment must be compatible with their monitoring. https://www.dhs.gov/megacenters Battle Creek MegaCenter: 269-565-9616. They may be contacted for current standards.
2) IDS should be integrated into the access control system when possible. Contact the physical security group to determine which solution is appropriate.
3) Interior doors leading to all alarmed areas (such as but not limited to appropriate OI&T spaces, pharmacy and police spaces) shall be tied into both he access control system and intrusion system if they are separate.
4) Greater of 1-year parts and labor warranty or manufacturer warranty with labor shall be included for systems managed by the OVAHCS starting on the turnover date.
5) If the lessor owns/manages the IDS, it shall be installed and monitored by UL certified entities and must comply with all Federal, VA, State and local regulations and requirements.

Duress:

1) VA Police staffed locations
    a. Lynx computer-based panic system shall be used in areas with VA computers.
    b. Physical Lynx panic buttons may be used if the area has no VA computers.
    c. Contact Physical Security to determine what licenses if any are needed.
2) Non VA Police staffed locations
    a. Lynx computer-based panic system is preferred. Notification of duress can be set so that all employees receive notification
    b. Please contact VA Police Physical Security for Lynx capabilities to determine if another solution is needed
3) Duress may also be integrated into the ePACS system instead of using Lynx if approved by Physical Security.
4) Physical Security shall be contacted to determine if Lynx licenses need to be purchased.

Key Management:

1) Traka Touch Pro Intelligent Electronic Key Cabinets.
    a. Key Cabinets shall be installed in all expansions, remodels, and new facilities.
    b. The size/model of the cabinet is dependent on the number of expected users/keys to be maintained in that Facility/Building/Area.
        i. Small locations and buildings may only require 1 key cabinet.
        ii. Medium and Large facilities shall have a key cabinet in each clinic and department.
        iii. Contact VA Police Physical Security who will coordinate with the VA Locksmith and other key VA personnel to asses how many key cabinets are needed and where they shall be located.
        iv. Key cabinets shall have power and data installed behind the cabinet
    c. Key Cabinets shall be managed via Traka Web v03.14.0001 (may be upgrading to a newer version).
    d. Key Cabinets shall be integrated into the LenelS2 access control system.
2) Contact Physical Security to determine what licenses if any are needed.
3) Expansion and remodel projects shall include managed key boxes unless they are deemed unnecessary by VA Police Physical Security.
4) VA Police Physical Security shall determine the appropriate key box size(s) and number of keys to be held in the key box(s) and per keys per key box.

Network and networked devices:

The electronic security systems shall be on an isolated network. The VA Locksmith will provide specifications and guidance on if switches need to be acquired. All copper ethernet cabling shall be red in color Cat6a or better and be in conduit unless otherwise approved by Physical Security. All cabling shall be labeled with the termination points on both ends. UPS's may need to be supplied if switches are needed. Contact VA Police Physical Security who will coordinate with the VA Locksmith to determine if additional switches and related equipment are needed for any project with electronic security system components. All devices shall be terminated in the appropriate telecommunications/OIT closet unless

specified otherwise. All networking equipment must be in a non-occupied secure space, typically a OIT or electrical closet.

1) Switches
    a. Copper switches shall be Cisco 9300-24/48H Network Advantage with C9300-NM-4M/2Y/8X uplink module with a base 1100W AC (or better power supply) or better. Contact the VA Locksmith for the appropriate switch model. All other switches must be approved by the VA Locksmith.
    b. Switches shall have modular or fixed uplinks.
    c. Switches shall have secondary 1100W AC or better power supplies.
    d. Switches shall be capable of a minimum 60 watts PoE, 90 watts PoE (PoE++, UPoE, etc…) is preferred. For projects requiring switches, the camera types to be installed shall determine if the full 90 watt PoE capability is needed. For switch orders, check with the VA Locksmith to determine PoE wattage needed.
    e. Fiber switches shall be Cisco 9300 series, check with VA Locksmith for the correct switch and configuration.
    f. Core switches, check with VA Locksmith for correct configuration.
2) Switches and other networked devices such as access control boards and workstations shall only be installed once the room is turned over to the VA and secured. Peripheral devices without onboard storage such as card readers and cameras may be installed in their final locations.
3) Alternate manufacturers or models require approval from the VA Locksmith and Physical Security.
4) Cabling
    a. Cat6a or better cabling shall be used for distances 294 feet or shorter.
    b. Fiber shall be used for distances over 294 feet.
    c. 2 cables shall be run for each end device in case of damage to the in-use cable.
    d. Cable shall be red in color.
    e. Cabling shall be labeled at both ends with the location of the other end.
    f. A service loop of appropriate length for the cable run shall be left at both end points. The service loop in the IT closet should be away from the patch or switch.
5) Media converters shall be provided when needed.
6) All devices capable of having dual power supplies (such as networking devices and servers) shall include both power supplies.
7) When connecting a device please ensure the networking link light comes on. Let the POC for the install know if this does not happen so we can troubleshoot. The most common issue is it is the port is not patched in the IT closet.

Door’s, gates and Hardware:

1) The VA Locksmith shall be consulted on all proposed door locking hardware to ensure it conforms with requirements and can be serviced by the Locksmith.
    a. Door lock Core shall be 7 pin Small Format Interchangeable Core (contact the VA Locksmith for that facility’s lock pin count).
    b. Door lock Brand and model shall be approved by the VA Locksmith.
    c. Approval is needed for all locks.
        i. All locks shall accept 7 pin small form factor interchangeable core.
        ii. All locks shall be Grade 1.

iii. Locking hardware shall be Sargent hardware.

2) All door hardware shall follow the PSRDM and associated appendices guidelines.
3) When at all possible, doors shall be pre-drilled for electric mortise or electronic panic hardware.
4) All sliding doors shall include electronic locks.
5) All exterior doors other than emergency exit only doors without door handles on the outside shall be controlled by the ePACS system.
6) All gates, including pedestrian gates and inbound side, shall be controlled by the ePACS system.
7) Electronic door locking hardware shall be "fail secure" (locked when no power is applied to lock) unless it is required to be "fail safe" (unlocked when no power is applied to lock) to meet emergency egress requirements. Documentation of code or legal requirement shall be provided when "fail safe" is required.
8) Electric Mortise locks shall be the preferred type of electronic lock. Electronic strikes where required/necessary by the PSRDM.
9) Doors on the ePACS must have door position sensors with request to exit sensors.
10) All perimeter doors for areas requiring intrusion detection shall have door position sensors connected to the intrusion system.
11) Pin pad type and other mechanical "cipher" locks are not allowed.
12) Electronic Panic hardware may be used when appropriate and approved.
13) Magnetic locks.
    a. Shall have a mechanical backup.
    b. Shall have key override switches installed on the nonsecure side.
    c. Shall have an override button on the secure side.
    d. Shall not be used for exterior doors for other than temporary emergency fixes.
    e. Should only be used for opposing doors.
14) Wireless automatic door opener buttons must be approved by VA Police Physical Security in coordination with the VA Locksmith.
15) Copies of keys.
    a. VA Police shall have override keys to all doors in accordance with VA handbook 0730 within all facilities including leased facilities if the space is inside the VA owned/leased perimeter. VA Police Physical Security shall determine what keys are needed in multi-tenant spaces.
    b. Master keys shall be provided to minimize the number of keys held by VA police.
    c. VA Police shall have a copy of all Special Key Different (SKD) keys that are not on the master key system.
    d. VA Locksmith shall be given all required information to make duplicate keys.

General

1) All work requiring access to a server or the network must be done by a person who has a VA Tier 2 background check and is certified in that system.
2) All work on/inside control panels must be done by a person certified in that system.
3) All work on "end" peripheral electronic security system devices must be overseen by a certified person. The certified person must be on site for projects. It is preferred the certified person be on site for warranty and service work, at a minimum they must be able to respond to the site and available via phone to the technician.
4) All work shall include "as-built" drawing with cable paths when new equipment is installed.

5) All guidance from the VA CFM TIL and other VA guidelines shall be followed. Waivers may be reviewed for approval when necessary.
6) Where able, all exterior devices (ie copper cable, fiber cable, card readers, cameras, ect…) shall have appropriate electrical surge protection on both ends. This should include on cable surge suppression and appropriate grounding/bonding at the device end.
7) All electronic security system cabinets shall be keyed for the Orlando VA not a generic manufacture key when possible.
8) All contractors working on these systems must have the appropriate certifications, IE Pelco VideoXpert Enterprise to work on the Pelco servers.
9) All contractors doing installation or service and maintenance must have completed the OSHA 10 hour construction safety course.
10) The contractor shall provide a "Competent Person" as defined by OSHA when applicable.
11) A contractor using a lift must have a lift certification.
12) All certifications shall be provided to the COR or VA Program/Project manager prior to starting work.
13) Background checks may be required at the discretion of the VA based on the type of work to be done by each person.
14) All new electronic security system cabling shall follow VA requirements for being in conduit. Waivers may be required if this cannot be met due to where it needs to be installed or budgeted.
15) This document and all reference documents establish minimum standards and shall be used in conjunction with the VA PSRDM, VA handbook 0730, CFM TIL Division 28 or their successors.

VA shall retain ownership of all components with onboard storage/memory even when installed by a lessor. Equipment that has network information such as an IP address shall be retained by the VA. Equipment that is removed and will be reinstalled shall be stored by the VA.

References are the minimum standards:

1) https://www.cfm.va.gov/til/dManual.asp#PSR Physical Security and Resiliency section
2) https://www.cfm.va.gov/TIL/spec.asp#28 Division 28 – Electronic Safety and Security
3) Camera/ePACS locations: https://www.cfm.va.gov/til/PhysicalSecurity/dmPhySecAppxB.xlsx
4) Door type location guide: https://www.cfm.va.gov/til/PhysicalSecurity/dmPhySecAppxA3.xlsx
5) Door type requirements: PSRDM - Appendix A2 Security Door Opening Schedule (va.gov)
6) Security door types: PSRDM Appendix A1-Security Door Types (va.gov)
7) VA Handbook 0730 http://www.va.gov/vapubs/search_action.cfm?formno=730&SortBy=Pub_Type_Desc
8) VA Police Physical Security may be contacted at VHAORLPOLICEPhysSecurity@va.gov