THE CITY OF DETROIT
DEPARTMENT OF INNOVATION AND TECHNOLOGY
STANDARDS FOR INFRASTRUCTURE AND EQUIPMENT

PURPOSE

This document is designed to serve as the CoD (City of Detroit) standards for network and security systems. The objectives below defined by the Department of innovation and Technology set the expectations and requirements for network and security systems deployed within the City of Detroit.

The DoIT Network Structured Cabling and Security System Standards (The Standards) serves as the master reference document of criteria for City of Detroit Department of Innovation and Technology.

All teams that are responsible for engineering, delivery, and operations of network services that need to identify or classify a network device must comply with this standard.

This document defines the technical requirements necessary to maintain optimum reliability and efficiency within a CoD facilities and computing centers.

To create a meaningful and well understood cross team standard for naming network devices throughout the City of Detroit /DoIT network.

Offer guidance on how to design video surveillance systems and access control systems that meet CoD specifications.

Provide a set of best practices and standards to be followed during the system implementation to ensure consistency, reliability, and security

Outline technical and functional standards for various security components and systems, such to ensure they are up to CoD specifications.

Lay out the requirements for video surveillance, access control and intrusion detection systems to maintain secure and controlled access to facilities and protect against unauthorized entry or activities.

Dictate the methods of network and system testing to maintain system integrity, performance, and security.

Outline the necessary permits and inspections required by law or policy, ensuring that all systems meet legal and safety codes.

Address Exceptions: Provide a protocol for handling exceptions to the standards, allowing for flexibility under certain conditions while maintaining overall security posture.

SCOPE

The Standards will be applied to the entire lifecycle of DoIT support infrastructure within every City of Detroit Facility. This includes, but is not limited to, planning, design, construction, operating, maintaining, repairing, restoring and modernization as well as the administrative activities that support these processes.

CoD supported infrastructure is defined as all passive telecommunications and information technology equipment, and supporting physical space and equipment, supporting:

- Information Transport Systems (ITS), including copper and fiber optic cabling.
- IT equipment and systems, such as servers, storage, network switches, and distribution hardware.
- Telecommunications spaces, which involve telecommunications rooms, entrance facilities, datacenters, and both horizontal and vertical distribution pathways.
- Telecommunications equipment and systems (local and wide area network, telephone, cable television, etc.)
- Physical security systems, including surveillance cameras, access control devices, intrusion detection systems, Video management systems (VMS), and other related security infrastructure.
- The physical infrastructure equipment and systems necessary to support the operations of active equipment, ensuring the required levels of availability and sustainability. Such infrastructure includes power and power distribution units (PDU), environmental conditioning and monitoring and bonding and grounding systems.

MATERIALS AND QUALITY OF WORK

All materials shall be new, never used, reused, reconditioned, or refurbished components. The electrical and physical properties of all materials, and the design, performance characteristics, and methods of construction of all items of equipment, shall be in accordance with the latest issue of the various, applicable Standard Specifications of the following recognized authorities:

- A.N.S.I. American National Standards Institute
- A.S.T.M. American Society for Testing Materials
- BICSI Building Industry Consulting Services International
- I.C.E.A. Insulated Cable Engineer’s Association
- I.E.E.E. Institute of Electrical and Electronics Engineers
- N.E.C. National Electrical Code
- N.E.M.A. National Electrical Manufacturer's Association
- TIA Telecommunications Industry Association
- U.L. Underwriters Laboratories, Inc. NFPA National Fire Protection Agency

STRUCTURED CABLING STANDARDS

CAT6 STRUTURED CABLING SYSTEM PRODUCTS

Current cabling standard for all installations is CAT6E (Plenum)

Any one of the following CAT6E structured cabling system products are acceptable

- Hubbell NEXTSPEED Cat 6 enhanced
- Superior-Essex NextGainCat6EX
- Leviton-BerkTek Lanmark-2000
- Belden Cat6e+ Premium 3613
- CommScope Uniprise CS37P Cat6E

PATCH CABLE COLOR CODE REQUIREMENTS (Patch panel and drop)

- Central City Sites – Central City patch cables are **Purple**
- Public Safety Sites – Public Safety patch cables are **Blue**

Wireless and Security (cameras, door access) patch cables are **Green**

- Fax lines and analog phone lines – **White**

FIBER CABLING REQUIREMENTS

- Multimode, 50 micron, OM4, LC-to-LC unless otherwise specified

NETWORK RACK REQUIREMENTS

Panduit (2-post): Part #R2PW

- Panduit PR2V Vertical Dual-Sided Manager: Part #PR2VD06
- 19" Wall Mount Server Rack Cabinet
- 12U (24"w x24"d x25"h)
- (600x600x635mm.) (WxDxH),
- Glass Door (1 PDU, 1 fan, 1 shelf, 4 feet, 2 brush cable entries

AT&T WAN CIRCUIT REQUIREMENTS

In situations where a AT&T WAN circuit is being installed, the following items are required to be installed

- A minimum 4' x 4' x ¾" fire-rated plywood backboard
- 110v NEMA 5-15R, 15 Amp 3-prong electrical outlet. A dedicated outlet is required to ensure the draw of electrical current not overload your system, blow a fuse, or trip a circuit breaker. The circuit must accommodate for a maximum of 95 Watts. Use of extension cords is not permitted.

- A new #6 ground wire bonded to an MGN or UFER Ground terminated to a Grounding bus bar

MANAGEMENT OF TELECOMMUNICATIONS CABLING

Proper cable management is necessary to enable optimal airflow through IT equipment (minimizing energy usage), to allow identification and management of cabling throughout the IT equipment lifecycle, and to minimize risks of damage to the networking system by minimizing opportunities for damage to cables, connectors, and conveyances.

EVALUATION FACTORS

Cable management allows appropriate airflow

Cables properly labeled to allow easy identification

Cable management is organized, logical, systematic, and aesthetic

IMPLEMENTATION REQUIREMENTS

Cable that is installed above a suspended ceiling must be supported per NFPA code requirements. Three choices are, conduits, cable tray or by J-hooks.

Cabling plants shall be planned to enable the installation of IT equipment. Install and utilize cable conveyances (cable trays, cable managers, and similar) in all IT installations. Free-run telecommunications cabling is NOT maintainable or sustainable and has a higher lifecycle cost than properly designed and installed cabling plant systems.

Cabling shall be run in horizontal, vertical, or overhead cable management systems where available. Procure and install cable management equipment when cabling installations need such to enable aesthetic, managed cabling outcomes.

Always plan the cabling path and manage the cabling installation, down to the level of the patch cable to the individual piece of IT equipment. Individual cables shall not be free run.

Individual cable lengths shall be selected appropriately for their purpose. Cable slack shall be managed with attention to installation criteria such as bend radius. Excessive slack indicates a poor choice of cable length.

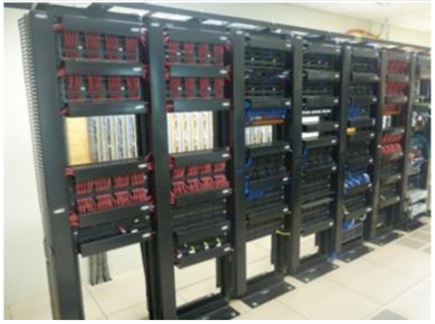
Patch cables and power cords between Rack PDUs and IT equipment shall not be run from one IT equipment rack to another. Power distribution detailed in the infrastructure section specifically calls out zone PDUs that supply power to multiple racks to obtain maximum power densities. These devices and their power supplies are not affected by this guidance.

Patch and power cables shall not be left unmanaged where they may interfere with exhaust airflow or have the potential to catch or snag on people or equipment.

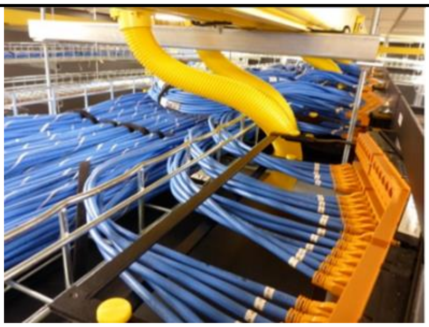
Document all cabling components and their linkage between components and make sure that this information is updated on a regular basis. The installation, labeling, and documentation should always match. Maintain cabling documentation, labeling, and logical/physical cabling diagrams.

EXAMPLES OF PROPER AND IMPROPER INSTALLATION

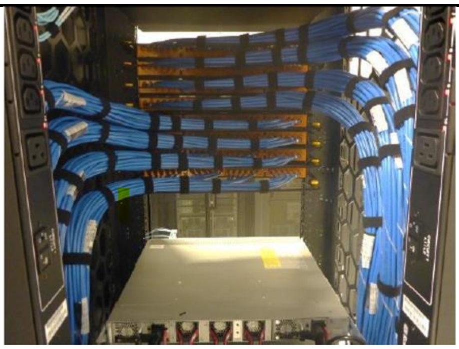
These are examples of acceptable cabling management implementations.



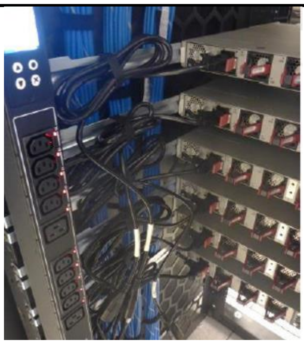
Proper management of patch cables with the use of horizontal and vertical wire managers



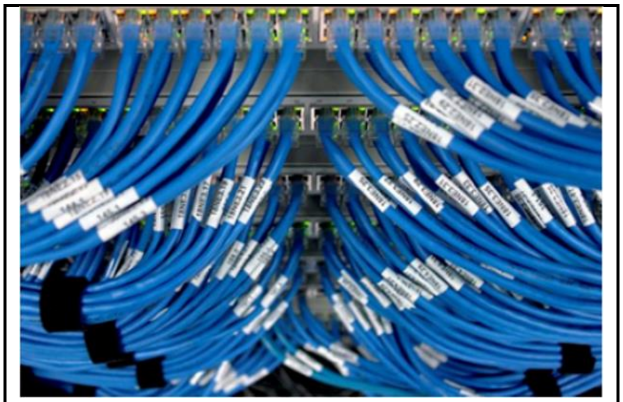
Properly dressed and labeled cables in a ceiling hung cable tray



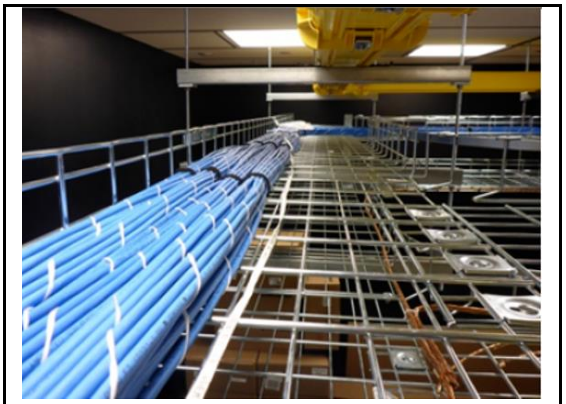
Properly dressed and organized cables in a server cabinet. Airflow is not obstructed, and cables are secured as to prevent damage



Cabling is carefully run as to not interfere with the sliding motion of the server or server cabling

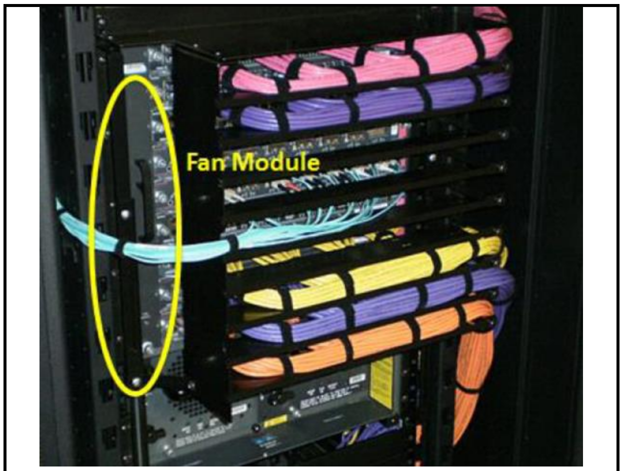


Ethernet patch cables neatly organized and labeled evenly and in-line with machine printed labels



Properly dressed cables in a ceiling mounted cable tray.

Consider vendor-specific IT equipment requirements for cabling so as not to impede intended operation of that equipment, such as blocking exhaust ports. The cabling management in Image 1 is appropriate except for the aqua-colored cables entering from the left, which cover the fan module on the left of the switch. This keeps the fan module from being replaced without disconnecting the network.



Aqua colored cables on the left are improperly installed as they prevent the removal of the fan module

INSTALLATION STANDARDS

Comply with latest editions and addenda of TIA-568 (SET) (cabling), TIA-569 (pathways), TIA-607 (grounding and bonding), BICSI N1, NFPA 70

Copper Clad Aluminum (CCA) twisted pair communication cable is strictly forbidden

All cabling shall be installed in a neat, workman like manner without twists, kinks, and unnecessary crossovers

Cables should not be in contact with the ground. Use cable management components and techniques to maintain a clean, clear, and safe work environment

Do not mount cabling in locations that block access to other equipment (e.g., power strip or fans) inside and outside the racks

Patch cables should follow the side of the IT equipment rack closest to the assigned NIC

Cables should not be looped around themselves or other objects

Route cables with gentle loops to avoid damage due to exceeding bend radius limitations. Glass fiber can be easily broken with rough handling or overly tight bends

Cables should be tight enough to maintain position but not tight enough to deform the jacket or put tension on the connectors

Based on heat exhaust (airflow), serviceability, and excess cable lengths, do not install folding/retractable cable management arms for IT equipment in computer spaces. Arms currently installed on existing equipment may be used until the equipment is refreshed and removed. · All cable slack should be concealed within the rack either vertically or within cable managers. Slack should not be looped. With use of the correct length cables, there should not be sufficient slack to enable looping. · Use the correct length patch cables. Cables should not be twisted or wrapped around other cables, including when bundled

NETWORK CABLE BUNDLING

Bundle cables together in groups of relevance (for example, cables to a single equipment distributor or uplinks to core devices), as this will ease management and troubleshooting.

Bundles of cables, when necessary, should be built from sub-bundles of no more than 16 individual cables. The larger bundles should not exceed 4 sub-bundles of like quantity.

When bundling or securing cables, use Velcro-based ties not more than every 1 to 2 meters, and more frequently as needed to maintain a clean installation. Do not use zip ties or twist ties for cable bundling or securing, as these apply pressure on the cables.

Only bundle like cable types. Do not bundle fiber, power, and UTP together.

Cable labels shall be visually accessible to local personnel following installation, for future Identification and troubleshooting purposes. Rather than bundling groups of cabling in a manner that prevents identification of individual cables, bundle in a different manner and/or relocate the cabling to locations where they will not be obscured. Consider bundling so all cables are on the exterior of the bundle.

UTP, FIBER, POWER CABLING

Segregate power and telecommunications cabling in separate cable tray systems; use different conveyance systems located not less than 12” apart when these two systems are run in parallel.

Where possible, run power and telecommunications in separate paths to reduce risks of EMI/RFI and data transmission losses.

Do not install UTP cabling on top of fiber cabling to prevent damage to the fiber transmission medium.

Segregate UTP and fiber telecommunications cabling, using different conveyances where possible. Where not possible or provided, ensure fiber cable is protected from damage. Use fiber inner duct where necessary within the same cabling conveyance.

Use properly sized equipment power cords; use of 6’ length power cords where 2’ cords are needed is not considered a best practice.

Separate A- and B-side power and segregate equipment power cords (between vertical rack power distribution units and IT equipment) by color for identification of A/B power to each piece of IT equipment.

CABLE LABELING

The CoD standard specifies use of ANSI/TIA 606-C compatible formats for identifying data communications cabling. More complicated installations may require reference to that document. Data communications cabling (UTP, fiber, and others) shall be labeled on both ends with information about the network port that it connects to on each end. Machine-printed tags secured with clear plastic or acetate adhesive tape are the minimum standard for these tags as in Figure below. Handwritten labels of any type are NOT permitted.

To identify the connected path of each data communications cable, the physical position identifiers at both ends of the cable are needed. The label for each end of the cable shall identify the six-digit drop ID as described on the next page/section of this document (**Drop and Patch Panel Labeling**)

DROP AND PATCH PANEL LABELING

All installed drops must be labeled and must correspond to patch panel labeling precisely according to the following specifications:

Patch panels should be labeled per the following specification: Each patch panel should be represented by a 3-digit alphanumeric label (e.g. 11A,21B, 31C) where the first numeric character represents the floor where the IDF/MDF exists (0 for basement, 1 for the first floor, 2 for the second floor, etc.) and the second numeric character represents the IDF number per floor. The third character is the unique letter designation for each patch panel beginning with "A". For example: The second of two IDFs on the first floor would have its patch panels labeled 12A, 12B, 12C and so forth. The actual patch panel ports should be labeled 001, 002, 003 and so on. Each patch panel port should begin at 001.

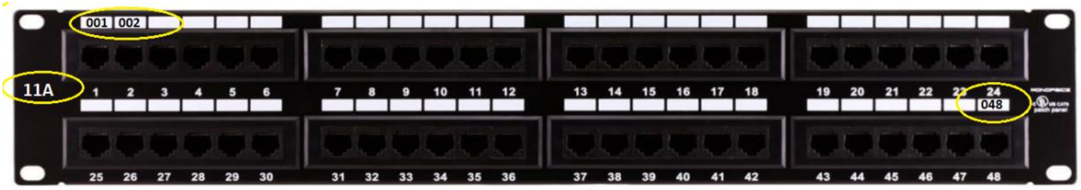
Drops (jacks) should be labeled per the following specification: The drop ID is a 6-digit alphanumeric name where the first three digits identify the floor, IDF and patch panel letter as explained in the patch panel labeling specification above, and the last three digits are numeric and represent the actual drop sequence number (001, 002, 036, 042 and so on). Drop ID numbers should match patch panel numbering.

Drop ID examples: Jack with 12A022 would indicate that the drop is on the 1st floor, terminating to IDF 2, patch panel A, and patch panel port 022. In another example, drop 21C010 would indicate that the drop is terminated to an IDF on the 2nd floor, IDF 1, patch panel C, and patch panel port 010. Note: Basement floors are denoted with a "0".

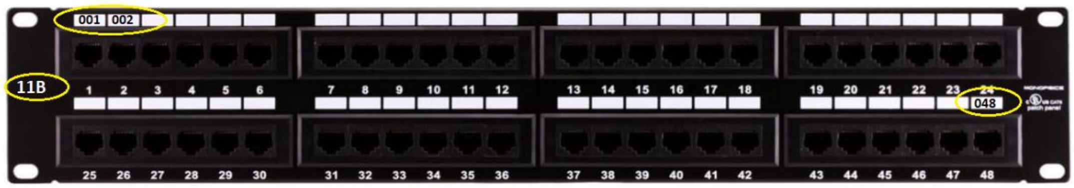
FIRST DIGIT	SECOND DIGIT	THIRD DIGIT	LAST 3 DIGITS
Floor	MDF/IDF	Patch Panel	Drop Sequence Number
1	**2**	**A**	**022**
2	**1**	**C**	**010**
0	**1**	**B**	**003**

Patch Panel labeling illustrated: Note: Patch panel **ports** must be labeled as shown below according to the 3-digit drop sequence number. Patch panel port sequence numbering should start at 001 and end at 024 or 048 (depending on patch panel size) for each patch panel installed.

The first 3 digits of the of the drop ID must be label on the left side of each patch panel installed as shown here



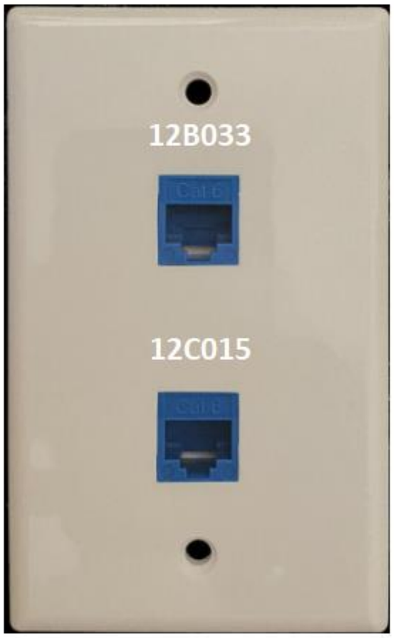
Corresponding jacks would be labled 11A001, 11A002, 11A048



Corresponding jacks would be labled 11B001, 11B002, 11B048

This new jack and patch panel lableling standard includes camera, and AP runs as well.

Drop (Jack) labeling illustrated:



First floor, IDF 2, patch panel B, patch panel port 33

First floor, IDF 2, patch panel C, patch panel port 15

PATCH PANEL TYPES

Fixed form factor patch panels **required**. Do use modular (keystone) type patch panels. Preferred patch panel brands include Panduit, Ortronics, Black Box, Leviton, Tripp Lite, and Hubbell

SECURITY VENDORS

COMPANY REQUIREMENTS

The company installing cameras, access control, intrusion detection or any other device connecting to the City of Detroit Genetec system must be a Genetec certified channel partner. Elite Certification or better is preferred.

Companies not Genetec certified may not sub-out to Genetec certified companies.

The company needs to have current certifications for the security hardware they are installing and must be able to create support requests as needed with manufacture for all components being provided.

EMPLOYEE REQUIREMENTS

The individual programming the Genetec system must have a Genetec Omnicast and Synergis Certificate for video/access control

All individuals working on any CoD Security and Network systems must be fingerprinted and background checked by the Detroit Police Department and have Michigan state police CJIS security awareness training on file.

Proof of clearance and certifications shall be provided prior to starting work

SECURITY SYSTEM DESIGN GUIDELINES

GUIDELINES FOR VIDEO SURVEILLANCE DESIGN

The following areas should be considered for coverage when designing a video surveillance system

- Building Ingress and egress areas
- Exterior perimeter of building and approaches
- Doors controlled by access control systems
- Elevator lobbies
- Stairwells
- Money handling or mail areas
- Front desk/customer interaction areas
- Special needs areas
- Areas where high value items are stored
- Rooms containing security system servers, access control systems, and intrusion systems controllers.
- IDF/MDF rooms where network switches are located
- Emergency call box locations

GUIDELINES FOR ACCESS CONTROL SYSTEM DESIGN

It is recommended the following areas be outfitted with access control doors as budget permits

- Perimeter doors
- high security areas
- restricted access rooms
- inventory and storage rooms
- MDF and IDF rooms
- Magnetic locking mechanism should be avoided whenever possible

GUIDELINES FOR VIDEO INTRUSION DESIGN

Intrusion points should include

- sensors on exterior doors and entry points
- motion detection on main entry points, 1st floor halls and corridors, rooms with windows reachable from the exterior, areas with valuables
- glass break sensors should be installed in areas with significant glass

SYSTEM IMPLEMENTATION REQUIREMENTS

All security designs and installations must be reviewed and approved by DoIT PS prior to procurement and installation.

All security system design and hardware submittals are approved by DoIT PS

Project kickoff includes communication plan involving all stakeholders

Prior to commencement of work, city project manager to coordinate activities and access to site, contractor, city project manager, DoIT network and DoIT PS must conduct mandatory job walk

CoD will validate all camera views. The camera aiming process must be coordinated and collaborated with the CoD

Existing installations, if the addition of new devices cause more that 80% of the open ports on the switch to be used, a new switch must be purchased.

Switch make and model to be approved by DoIT Network team

Programming shall not start until Genetec licenses for the project are purchased and loaded into the CoD Genetec system

Vendor laptops are not allowed to be plugged into CoD network Switches. All Genetec programming must occur through the CoD Securelink system. Camera programming must occur through SecureLink via the on-site archiver or via standalone vendor supplied network / POE hardware.

After a site is commissioned and handed over to the customer, all vendor access and entry to the site must be scheduled and coordinated with DoIT

VMS

GENETEC VMS SYSTEM STANDARDS

The CoD uses Genetec as its enterprise security system. No other type of security systems is allowed to be installed on the CoD network.

The CoD requires all security systems to be installed as an expansion to the current system.

All installed expansion instances of the Genetec server software must be version 5.10.2129.0

Locations with surveillance cameras shall have a Genetec Streamvault archiver installed on site.

Streamvault SV350 or larger are allowed. SV300s are not allowed.

Archiver shall support 30 days of continuous recording video on all cameras using CoD supplied cameras settings

Archiver primary video storage shall be configured in a redundant RAID configuration

Archiver must be rack mounted and locked in cabinet

Non-rackmount archivers shall be provided with official genetec rack mounting accessories

Archiver shall include rackmount KVM

Archiver shall have a remote management NIC (iDrac or iLO). Remote management system shall be confirmed as per DoIT specifications.

Archiver shall be protected by UPS. Model of UPS to be confirmed by DoIT

Archiver UPS shall be connected to network for monitoring, programmed with IP provided by DoIT

CoD camera settings will be supplied at the start of project

Whenever a camera is in view of a door that is access controlled. That camera shall be associated with that door

Whenever possible, a drawing of the building shall be entered into Genetec maps, and the appropriate doors and cameras overlaid onto that map

SECURITY CAMERAS

SECURITY CAMERA STANDARDS

The CoD uses AXIS Cameras exclusively for video surveillance. Any other types of video surveillance cameras are not allowed to be installed unless explicitly allowed by DoIT

All camera models must be certified to work on Genetec version 10.5.2

AXIS Cameras shall be P or Q series. M series for fisheyes style cameras only.

Refer to section x.x "APPROVED HARDWARD SPECIFICATIONS"

Allowed M series cameras: M43

Allowed P series cameras: P13, P14, P32, P373x, P38, P47

Allowed Q series cameras: Q16, Q17, Q35, Q36, Q60-63, Q87

Any variations to the above must be approved by DoIT PS

AXIS Cameras shall have advanced object detection

Cameras are mounted with AXIS compatible mounting systems.

Cable penetrations into the camera body utilize the AXIS supplied cable gaskets. Gaskets must be installed and in good condition.

Network camera drops are terminated at the camera side into a labeled jack

Network cameras shall be connected to the jack with vendor supplied green patch cord

Camera installation does not occur until construction activities have completed (drywall, painting)

All cameras mounted to a drop ceiling are to be secured with a solid support within or above the tile. No direct mounting to ceiling tiles is allowed

IP based door intercoms must be compatible with Genetec

All cameras must be labeled with an electronically printed label, The label shall be black on white for white cameras and be 1" inch tape height. The label text shall match what is provided by the DoIT hardware sheet

ACCESS CONTROL

ACCESS CONTROL SYSTEM REQUIREMENTS

All card readers deployed must support PROX, iClass, and Bluetooth technologies

Door controllers, readers, operators, sensors and accessories must be secured with a reliable source of emergency power to guarantee functionality during any power interruption scenarios

Door controllers shall be centralized to the building or floor, not installed at door location unless authorized by DoIT

All door controller units shall be Mercury LP series and MR series 3 boards

Each location utilizing mercury door controllers should have 1 Genetec cloudlink installed on site.

When the current demand for the door hardware exceeds the capacity of the door controller, an auxiliary power relay shall drive the door hardware.

HID EDGE EVO controllers are not allowed

All doors shall have an unlocking device, REX, and door contact (door sensor)

2N Card readers are not allowed

If required per code, the access control system shall interface with the fire alarm system to ensure in the event of fire alarm activation of system failure access-controlled egress doors are released to allow unobstructed exit.

All cabling used for connecting door controller hardware to controllers shall be composite in nature, combining power, data, and other functions in a single sheath.

All exposed cabling shall be routed withing conduit to provide against physical damage,

Communication and equipment room cabling shall be routed within conduit, slotted cable duct, or coverable cable raceways.

Access control cabling shall be organized neatly and tidily to facilitate east identification, maintenance, and troubleshooting. All cables shall be supported, dressed, and labeled.

INTRUSION DETECTION

INTRUSION DETECTION SYSTEM REQUIREMENTS

Intrusion detection panel shall be Bosch model B9512G unless otherwise approved by DoIT

Panel and all accessories must be powered by backup batteries in the case of primary power loss

Network connectivity via CAT6 cable that is run to the panel enclosure and terminated at a labeled keystone.

Each Motion detector, glass break sensor, and door and window contacts are addressed as unique points

Intrusion system can detect physical tampering, including opening of the panel enclosure.

System is integrated into the CoD Genetec system, appropriate licenses are purchased to do so.

User pin codes are synced to Genetec via Cardholder credentials

On site sirens audible alert individuals in the case of intrusion system activation. Both interior and exterior sirens should be considered.

Individual Genetec alarms are created for each point or similar group of points as authorized by DoIT

System allows 60 seconds to exist prior to arming and 45 seconds to disarm post entry

All detection devices, including motion detectors, glass break sensors, and door and window contacts trigger and immediate alarm, except if those sensors are triggered by the entry of a person disarming the system.

Panel password and configuration is made available to the CoD

All points are tested and confirmed to operate as expected prior to commissioning of the system.

All exposed intrusion system cabling shall be routed withing conduit to provide against physical damage

Communication and equipment room cabling shall be routed within conduit, slotted cable duct, or coverable cable raceways.

SYSTEM TESTING

NETWORK TESTING REQUIRMENTS

All copper drops must be certified utilizing a device designed to certify according to TIA/ISO standards. Some examples include Fluke Networks DSX, AEM TestPro CV100, and VIAVI Solutions Certifier. The certification report shall be provided to the COD in electronic format.

Fiber optic cable shall be tested with a calibrated OLTS or OTDR appropriate for the fiber type and wavelength under test

Report of test results shall be provided to DoIT at the end of project

CLOSEOUT AND DOCUMENTATION

DOCUMENTATION REQUIREMNTES

As-builts provided at end of project shall include:

- Hardware cut sheets and user manuals
- Warranty information
- Hardware inventory report in CoD Format
- Drawings showing cable pathways, device locations
- System test reports

COD HARDWARE INVENTORY

The following vendor supplied information shall be included on the hardware inventory report

- Device type (camera, door, intrusion, server, other)
- Device makes
- Device model
- Device location
- Device name
- MAC Address (if applicable)
- Temporary device credentials

PERMITS AND CODE INSPECTION

COMPLIANCE WITH BUILDING CODES

All projects must adhere to local, state, and federal building codes.

Prior to commencement of work, the appropriate low voltage and electrical permits must be obtained by the city of Detroit BSEED

Inspections must be scheduled with the CoD BSEED and passed prior to completion

APPROVED HARDWARE SPECIFICAITONS

1.1. TBD/WIP

EXCEPTIONS

All exceptions under this standard must be submitted in writing and approved by the City of Detroit Department of Innovation and Technology

DEFINITIONS

- BSEEED = CoD Buildings, Safety, Engineering, and Environmental Department
- CAT6 = Category 6 standard for twisted pair cable
- CoD = City of Detroit
- DoIT = Cod Department of Innovation and Technology
- DoIT PS = Public Safety
- DROP = a run of communication cable from the network switch to the connection point where a device is connected to the network
- MGN = Main Grounding Neutral
- OLTS = Optical loss test set
- PDU = Power distribution unit
- REX = Request to Exit Sensor
- UFER = Concrete encased electrical ground
- UTP = unshielded twisted pair
- VMS = Video Management System

REFERENCE STANDARDS

- BICSI N1 - Installation Practices for Telecommunications and ICT Cabling and Related Cabling Infrastructure, 1st Edition; 2019.
- EIA/ECA-310 - Cabinets, Racks, Panels, and Associated Equipment; Revision E, 2005.
- NFPA 70 - National Electrical Code; Most Recent Edition Adopted by Authority Having Jurisdiction, Including All Applicable Amendments and Supplements.
- TIA-568 (SET) - Commercial Building Telecommunications Cabling Standard Set; 2019.
- TIA-568.2 - Balanced Twisted-Pair Telecommunications Cabling and Components Standards. 2009c, with Addendum (2016).
- TIA-569 - Telecommunications Pathways and Spaces; 2019e.
- TIA-606 - Administration Standard for Telecommunications Infrastructure; 2017c.
- TIA-607 - Generic Telecommunications Bonding and Grounding (Earthing) for Customer Premises; 2019d.
- UL 444 - Communications Cables; Current Edition, Including All Revisions.
- UL 514C - Nonmetallic Outlet Boxes, Flush-Device Boxes, and Covers; Current Edition, Including All Revisions.
- UL 1863 - Communications-Circuit Accessories; Current Edition, Including All Revisions.