STATE OF DELAWARE
DEPARTMENT OF TECHNOLOGY AND INFORMATION
801 Silver Lake Blvd.
Dover, Delaware 19904

Doc Ref Number:	SE-VideoSurv-001	**Revision Number:** 2
Document Type:	Enterprise Policy	**Page:** 1 of 8
Policy Title:	Video Surveillance Policy	

Synopsis:	The goal of this policy is to establish the permissible uses and technical specifications for the State's Video Surveillance Information.
Authority:	Title 29 Chapter 90C Delaware Code, §9004C – General Powers, duties and functions of DTI "2) Create, implement and enforce statewide and agency technology solutions, policies, standards and guidelines, including as recommended by the Technology Investment Council on an ongoing basis and the CIO"
Applicability:	This policy is applicable to all users of the State of Delaware communications and computing resources. The Department of Technology and Information (DTI) is an Executive Branch Agency and has no authority over the customers in Legislative and Judicial Branches, as well as Local Education Agencies, and other Federal and Local Government entities that use these resources. However, all users, including these entities, must agree to abide by all policies, standards promulgated by DTI as a condition of access and continued use of these resources.
Effective:	4/1/2024
Reviewed:	4/1/2024
Approved By:	Chief Information Officer
Sponsor:	Chief Security Officer

TABLE OF CONTENTS

Section		Page
I.	POLICY	2
II.	DEFINITIONS	4
III.	DEVELOPMENT AND REVISION HISTORY	4
IV.	APPROVAL SIGNATURE BLOCK	5
V.	LISTING OF APPENDICES	5

I. POLICY

EXECUTIVE SUMMARY

This policy sets forth the permissible uses for video surveillance, including mandatory technical specifications for all video surveillance deployed by and within the State.

PURPOSE

The increased availability of surveillance devices and cameras has raised questions concerning their appropriate use, particularly inside the workplace. Video surveillance systems procured by the State must maintain minimum security specifications to ensure the safety of State employees, facilities, and data. This policy regulates all uses of surveillance cameras and surveillance monitoring and recording in order to achieve these purposes while also protecting the legal and privacy interests of the State, its citizens, and employees. Excluding law enforcement, only State authorized surveillance equipment is allowed to be used for surveillance. The use of personally owned surveillance equipment is thereby prohibited from being used for surveillance of any nature.

POLICY

1. Physical access doors and gates into a facility with connectivity to the State computing network must be monitored by a video surveillance system around the clock; 24 x 7 and 365 days a year.
2. Video surveillance systems monitoring access to State facilities must store and maintain at least 90 days' worth of recorded activity.

3. Video surveillance systems monitoring access to State facilities must have night vision capability and produce reasonably clear captures of activities.
4. State secure facilities with controlled gate access must implement Automatic Number Recognition (ANPR) capable camera systems at the gate entrance with direct site of entering vehicles, where possible.
5. DTI will partner with all affected organizations, Facilities Management, and the Department of Safety and Homeland Security (DSHS) to oversee the implementation of this policy.
6. The decision to install such a system should be made by the Agency, based upon a risk assessment of the operations being conducted at that facility location. Any proposed systems or services must comply with the State's Video Surveillance Policy, which will ensure consistent and secure usage of surveillance across State facilities, excluding schools and correctional institutions. Agencies are reminded that the responsibility for funding and maintenance of a video surveillance system exists at the Agency and Department level and is not a responsibility of DSHS, Office of Management and Budget (OMB), or DTI.
7. The system must comply with National Electric Code.
8. The use of surveillance equipment is limited exclusively to practices that will not violate the standard of a reasonable expectation of privacy and protection of sensitive information as defined by law. Any cameras not meeting or exceeding these requirements shall be removed.
9. Surveillance equipment specifications will adhere to the technical specifications published within this policy in Appendix A.

ENFORCEMENT and WAIVER

DTI will enforce this policy during the course of normal business activities, including business case and architectural review of proposed projects and during the design, development, or support of systems. This policy may also be enforced by others during the course of their normal business activities, including audits and design reviews. In the event a proposed system or equipment does not align with requirements, the requesting agency should pursue an exception through the DTI waiver process.

If there is ambiguity or confusion regarding any part of this policy, contact the sponsor named in the header of this policy.

II. DEFINITIONS

1. **Surveillance Equipment/Security Cameras** — any item, system, camera, technology device, communications device, or process, used alone or in conjunction with a network, for gathering, monitoring, recording, or storing an image (s) of State property and/or people on State property. Video surveillance is also referred to as CCTV.
2. **Network Video Recorder (NVR)** – A computer system that records video footage and stores it on a hard disk, a mass storage device or cloud storage. They are paired with digital internet protocol (IP) cameras to create video surveillance systems.
3. Types of equipment include:
    - ✓ Security Cameras which can be either IP-Cameras or Analog Cameras
    - ✓ A Recording and Monitoring solution:
        - In small systems recorders are used. Recorders can be distinguished in Network Video Recorders
    - ✓ Outdoor surveillance cameras – includes night-vision features.
    - ✓ Motion -activated surveillance cameras- starts recording once motion is detected.
    - ✓ Biometric surveillance – Biometrics are unique physical characteristics, such as fingerprints, facial, voice, iris and/or palm patterns (includes key card with picture identification). Iris recognition is considered one of the most secure biometric methods due to the uniqueness and stability of iris patterns.
    - ✓ Wireless/Internet cameras -real-time monitoring
    - ✓ Security System cameras

III. DEVELOPMENT AND REVISION HISTORY

Date	Revision
8/15/2014	Rev 0 – Initial version
12/21/2015	Rev 1 – Updated content related to surveillance video
4/1/2024	Rev 2 – Significant update to the retired policy

IV. APPROVAL SIGNATURE BLOCK

On File	
Name & Title:	**Date**
State Chief Information Officer	4/1/2024

V. LISTING OF APPENDICES

Appendix A

The following are minimum requirements of the IP Video Surveillance Systems in State of DE facilities:

ONVIF Compliance

ONVIF Compliance ensures that regardless of manufacturer, an IP Camera will be compatible with devices from other manufacturers.
ONVIF Certified products can be identified using the ONVIF conformity tool.
https://www.onvif.org/conformant-products/

- Must be compliant with ONVIF profile/s S and/or T.
- For Devices that support onboard recording to an SD card ONVIF Profile G is recommended.
- All other ONVIF profiles optional.
    - S – Supports compatibility between Network Video Recorders and Video Management Systems. Also includes ONVIF specifications for Pan Tilt Zoom (PTZ) control, audio, multicasting, and relay outputs for conformant devices and clients that support such features.
    - G – Supports replay controls and Edge Storage allowing the option of storing recordings on camera via SD card

- T – Supports H.264 and/or H.265 encoding which lowers bandwidth and storage requirements for footage. Also supports encrypted HTTPS protocol. (Not yet finalized, currently in Release Candidate phase.)
- Additional ONVIF Profiles and information can be found here: https://www.onvif.org/profiles/

Security Features/Requirements

- All cameras must be Encrypted via HTTPS protocols TLS 1.2 (preferred), TLS 1.3 (emerging).
  - Ciphers should be AES 128 bit or higher.
  - ECDHE is also approved for use.
- Must support multi-level passwords.
  - At a minimum must support Administrator and Single User password.
- Camera management systems that provide web-based or client-based access to one or more cameras must adhere to the State Identity and Access Management policy.
- Local or remote access to camera management systems that provide access to one or more cameras must leverage the State's identity solution and enable the management of access through an approved user's lifecycle with the state or associated role.
- IP Cameras that have passwords set by the manufacturer, that cannot be changed, are not authorized.
- Cameras may not use default passwords. All passwords must meet the complexity requirements set in the State Identity and Access Management Policy
- Camera software and firmware must be upgradable without direct internet access to the devices. It is suggested that software and firmware packages be downloaded from an internet connected machine and placed in a location accessible by the Camera Management and/or NVR software.

Resolutions

- **Minimum Resolution 720p**
  - 1280x720(720p) at minimum of 15 Frames per Second (FPS)
  - Should only be considered for applications below 15ft from subject if device **does not** feature an **optical** zoom lens.
- **Recommended Resolution 1080p**
  - 1920x1080(1080p) at minimum of 15 FPS, 30FPS Preferred.
- **Higher Resolutions**
  - Considerations should be made when going above 1080p, to ensure storage and network bandwidth is sufficient.

- Table 1 contains estimated storage and bandwidth requirements.
- Values can be halved if cameras are set to record only on motion or record non-motion at a lower quality. This can offer a considerable cost savings.

Resolution	Width	Height	Estimated 30 Day Storage at 15 FPS	Estimated Network Bandwidth at 15FPS
4K	3840	2160	4490 GB/4.49TB	12.0 Mb/s
2K	2048	1566	1650 GB/1.65TB	4.88 Mb/s
1080P	1920	1080	885 GB	2.61 Mb/s
720P	1280	720	451 GB	1.34 Mb/s
480P	854	480	NA	NA

Table 1 –Resolutions and H.264 Storage and Network Bandwidth Estimates

NVR Storage

- NVRs should be sized for a minimum of 90 days of storage for the devices managed by it.

Video Encoding

- NVRs must support H.264 and/or H.265 encoding formats.
- NVRs must Support Motion JPEG (MJPEG) if legacy IP Cameras exist in your implementation.
- Proprietary video formats may only be used if the NVR or Video Management Software (VMS) also supports one of the formats above and can export the video to a commonly utilized open format.

Power Requirements

- Power over Ethernet requirements (PoE) must be determined by the network device the camera will be utilizing, the number of other cameras utilizing PoE on the same network device, and the distance from the network device.
- Type 1 and Type 2 devices are preferred as they are more widely supported.
    - Type 1 PoE IEEE 802.3af
    - Type 2 PoE+ IEEE 802.3at
- In some cases, add-on PoE power supplies may be required.
- NVRs and Network Devices which power IP Cameras, must have Uninterruptable Power Supplies (UPS) in place to ensure camera functionality in the event of a power outage.

Network Requirements

- Devices must be able to function without connectivity to the internet.
- Devices must reside within a designated security network with isolation from internet access and the internal user network. All inbound and outbound access must be implemented through a State firewall and approved by the DTI Chief Security Office.
- Camera systems outside the State defined requirements must be approved by the Chief Security Office within DTI, before purchase via the DTI waiver process.

Environment Specific Requirements

- Cameras exposed to weather elements must be rated for outdoor use.
- Pan Tilt Zoom (PTZ) Cameras that are exposed to freezing temperatures must be rated for arctic/freezing temperatures.
- Where cameras may be exposed to high levels of humidity, defogging lenses are recommended.
- Cameras that can be easily reached by inmates must be rated as Vandal Resistant or provide Active Tampering notification.
- Cameras used in low light applications should have built-in Infrared (IR) capabilities.