

# Network Connections for Surveillance System Cameras and Digital Video Recorders Policy

## **POLICY:**

The Darton College network infrastructure may serve as a distribution means for digital information collected by surveillance camera systems and associated recording devices that are primarily used for obtaining identifiable personal images. Connection of IP addressable cameras and digital video recorder systems used for this purpose to the Darton College network (either through direct copper/fiber wiring or indirect 802.X technology) must be approved by the College Chief Information Officer (CIO) and the Network Support Specialist prior to being placed in operation.

## **Rationale:**

Increased attention to security and protection of human and physical resources around the Darton College campus has resulted in need for quickly deployed and easily maintained security and surveillance systems. Digital recording devices and digital monitoring devices provide a very cost effective solution and are readily available. However, placing these devices on the data network without proper information security consideration or configuration could result in access to the system or to information being collected on the system by unauthorized users. This is particularly critical for systems that are either protecting valuable resources or for systems that may collect evidentiary information for future prosecution of suspects. In order to ensure systems are being accessed only by the minimum persons required, equipment and software must be reviewed by the CIO and network staff to determine if the requested system can be secured, methods that can be used to access the system from on and off campus, and potential impact on network traffic when the system is placed in service.

## **Standards & Procedures:**

### **Standards:**

**Denial of Access.** IP addressable cameras and IP addressable digital video recorders (DVR) (associated with either analog or digital cameras) making a physical or 802.X connection to the College network infrastructure must allow for denial of access by other than those users specifically included in a system Access Control List (ACL).

**Access through VPN.** All access to IP addressable cameras and associated digital recorders used for security and surveillance from other than physical connections to the campus network will be accomplished through the centrally managed Virtual Private Network (VPN).

**Audit Reporting of Accesses.** Digital video recorders used to collect and store identifiable personal images should be configurable to allow audit reporting of accesses to the recorder.

**Evidentiary Documentation.** Digital video recorders used to collect and store identifiable personal images should include technology for "watermarking" of files in order to be suitable for evidentiary documentation.

**Systems Accessed by Darton Policy Personnel.** Security and surveillance camera systems that are intended to be accessed by Darton College Security personnel will comply with the following technical specifications:

- Allow for simultaneous viewing of live and recorded images
- Store recorded images in MPEG II format
- Include capability for transfer of stored images to external storage media
- Does not require vendor specific/proprietary applications or clients for viewing live or stored images
- Provides 7 days of image storage from all connected cameras on the recording device

**Procedures:**

[Register Internet Services Devices \(Servers\)](#)

*Digital Video Recorders are classified as “servers” and must be registered in accordance with College Policy.*