The Board of Trustees of the Columbus Metropolitan Library (CML) is responsible for establishing rules to maintain security and safety for members of the public and CML employees. As part of that responsibility, this policy is established to regulate the use of CML video surveillance. Video surveillance is intended to observe and record areas on the premises of CML for safety and security purposes, including for the protection of CML, its employees, customers and contractors against attack, interference or sabotage. This policy applies to all employees and contractors of CML in the use of CML video surveillance and recording. The existence of this policy is not intended to, nor does it, imply or guarantee that: (i) any or all cameras will be recording images, or monitoring in real time, 24 hours a day, seven days a week, or (ii) use of cameras will be effective in preventing, or identifying the perpetrators of, attacks or criminal acts.

Scope

1. Video surveillance for security purposes is limited to areas that do not violate the reasonable expectation of privacy. Such areas may include public spaces, staff work areas, parking lots and grounds.
2. Targeted video surveillance is prohibited if such observation is based on characteristics and classifications that would be considered discriminatory under law (e.g., race, gender, sexual orientation, national origin, disability, etc.).
3. Video surveillance for security purposes will be conducted in a professional manner. Personnel involved in video surveillance will be trained in its responsible use. Only select personnel will be permitted to view surveillance footage, save or retain such footage outside of CML’s standard retention period and practices, and release such footage to law enforcement or other outside parties.

Administrative Procedure:

A. Responsibilities and Permissions
CUSTOMER POLICIES

1. The Director of Security has sole authority with respect to the installation, orientation, relocation, replacement and use of all camera surveillance for safety and security purposes. Cameras cannot be installed, relocated or reoriented without the approval of the Director of Security.

2. The Director of Security responds to recommendations, complaints and concerns regarding camera locations. The Director of Security reviews camera locations to ensure the viewing area of cameras conforms to this policy and procedure.

3. The Director of Security or their designee reviews and coordinates responses to all requests received from law enforcement for footage and images obtained through video surveillance. The Director of Security or their designee may release video footage and images to law enforcement personnel acting within the scope of their official duties upon request, provided such release does not disclose customer library records or customer information as described in the Confidentiality of Customer Library Records policy.

4. Video surveillance footage and images may also be released by the Director of Security or the Risk and Compliance Manager under the following circumstances:
   i. In response to a request related to investigation of an insurance claim;
   ii. In response to a subpoena, search warrant or court order;
   iii. In response to other requests in accordance with the Public Records Request policy and provided such release is permitted under the Confidentiality of Customer Library Records policy.

5. All subpoenas, search warrants, court orders and related documents must be submitted to the Risk and Compliance Manager.

6. Subject to the requirements of the Confidentiality of Customer Library Records Policy, CML employees may allow law enforcement personnel to view recorded or live video surveillance at a CML location when exigent circumstances exist. However, all requests for copies of footage and images from law enforcement must be referred to the Director of Security or their designee as documented in item #3 above.

7. Requests for video footage and images from anyone other than law enforcement (e.g., members of the public, media, etc.) must be referred to the Risk and Compliance Manager as a public records request. The Risk and Compliance Manager will follow the public records request process in responding.

8. Photographs and digital images of individuals obtained through video surveillance should not be displayed in an area that can be viewed by customers without prior authorization by the Director of Security.

9. CML employees may attach images obtained from video surveillance to incident reports to aid in the identification of suspended and/or potentially dangerous individuals. Images obtained from Video surveillance may also be used internally for “be on the lookout” (BOLO) or similar messages shared within CML.
CUSTOMER POLICIES

10. Temporary cameras with recording equipment may be used for investigations by CML’s Security department. The Director of Security must approve such camera use prior to installation. In the event that the Director of Security is the subject of an investigation, such camera use must be approved by the Chief Diversity, Equity and Inclusion Officer.

B. Recorded Video Retention

1. Recorded video obtained through video surveillance will be automatically erased seven (7) days after recording, unless retained as part of a criminal investigation, court proceedings, or other bona fide use as approved by the Director of Security or their designee.

2. Video footage retained as part of a criminal investigation, court proceedings, or other bona fide use will be stored in a secure location by the Director of Security or their designee.

Related Policies/Forms:

- Confidentiality of Customer Library Records
- Customer Code of Conduct
- Suspensions