Video Surveillance Policy

The Trustees of the Berkshire Museum (herein "Museum") are committed to the enhancement of public safety, the quality of life, and the maintenance of an environment conducive to conducting Museum business. Accordingly, the Museum is using closed ‐circuit television (CCTV), which includes video surveillance cameras, monitors and digital video recorders, to monitor public areas in order to deter crime and assist the Pittsfield Police Department (PPD) in providing for the security and safety of individuals and property of the Museum.

The PPD shall not collect or maintain information about members of the community (employees, residents, or visitors), except in connection with alleged crimes, violations of Museum regulations, or as specifically authorized in writing by the Executive Director of the Museum.

Purpose

The purpose of this policy is to provide guidelines for the use of CCTV on Museum property in a way that enhances security, while at the same time respects the expectation of reasonable privacy among members of the community and Museum employees. Further, this policy is intended to formalize procedures for the installation, monitoring, store, dissemination and destruction of surveillance records. All Museum departments or units using CCTV and web camera surveillance are responsible for implementing this policy in their respective operations.

The existence of this policy does not imply or guarantee that security cameras will be monitored in real time continuously or otherwise.

Entities Affected by this Policy

All Museum employees, as well as visitors to Museum offices/departments, are covered by this policy.

Definitions

These definitions apply to these terms as they are used in this policy:

CCTV: Closed circuit is a technology that can be used to remotely monitor and record activity throughout Museum office spaces and buildings. CCTV (closed---circuit television) is a TV system in which signals are not publicly distributed but are monitored, primarily for surveillance and security purposes.

CCTV relies on strategic placement of cameras, and observation of the camera's input on monitors somewhere. Because the cameras communicate with monitors and/or video recorders across private coaxial and/or Ethernet wire cable runs or wireless communication links, they gain the designation "closed-circuit" to indicate that access to their content is limited by design only to those able to see it.

Forensic Video Surveillance: The scientific examination, comparison, and/or evaluation of video in and for legal and/or criminal matters.

Public Area*:* An area open for public use where the expectation of privacy is not violated by what could normally be openly observed, such as a Museum gallery, hallways, entrance, etc.

Private Area*:* Areas where an individual might change clothing, such as bathrooms, shower areas, locker and changing rooms. This would also typically include private office spaces; however, exceptions are appropriate in those areas where monetary transactions occur or where the use of CCTV is needed to safeguard money or supplies from theft, destruction or tampering.

Video Surveillance Technology*:* Any item, system, camera, technology device, communications device, or process, used along or in conjunction with a network, for the purpose of gathering, monitoring, recording, or storing an image or images of Museum facilities and/or people in Museum facilities. Images captured by video surveillance technology may be real-time or preserved for review at a later date. CCTV is one form of video surveillance technology.

Scope of Policy

This policy applies to all Museum personnel, including employees (full or part time, temporary, seasonal), interns, contractors, residents and visitors. This policy encompasses all use of video equipment for the purpose of surveillance on or in any Museum property, building, and spaces.

1. Exclusions

This policy does not apply to video used by or for:

Non-surveillance purposes. Examples of non-surveillance video recordings include, but are not limited to, video recordings made for:

a. Capturing public events and performances
b. Recording promotional or news events
c. Convenience such as weather or construction site viewing
d. Video conferencing
e. Requests from law enforcement.

2. Overview

The Museum recognizes the need to strike a balance between an individual's right to be free from invasion of privacy and the Museum's duty to promote a safe environment for all employees, residents and visitors. In light of this recognition, the Museum will use CCTV to enhance security, safety and the quality of life by integrating the best practices of "virtual policing" with CCTV technology.

And, while not a guarantee of safety, CCTV is a tool that can be used to assist Museum personnel. The purpose of CCTV surveillance is three-fold:

a. To promote a safe environment by deterring acts of harassment or assault;
b. To deter theft and vandalism and assist in the identification of individuals who commit damage to Museum property;
c. To assist law enforcement agencies with regard to the investigation of any crime that may be depicted.

Video monitoring for security purposes will be conducted in a professional, ethical and legal manner. Personnel involved in active video monitoring will be appropriately trained and continuously supervised in the responsible use of this technology. Violations of procedures for video monitoring referenced in this policy will result in appropriate administrative and/or disciplinary action consistent with the rules and regulations governing employees of the Museum.

3. Principles and Rationale

The Museum is committed to protecting the safety and property of our community by promoting a secure campus environment while avoiding unnecessary intrusions. This policy is intended to assure the appropriate use of video surveillance for reasons of safety, security, and stewardship of people and resources and provide transparency in the use of that technology/equipment. Video surveillance will be used in a professional and ethical manner in accordance with Museum policies as well as related local, state, and federal laws and regulations.

The Front of House and Facilities teams will monitor the application of this policy to new and existing uses of video surveillance; to create operational procedures related to the approval of requests, retention of and access to video surveillance footage, use of signage; and to provide for timely reviews of this policy.

4. Facial Recognition Software

The Museum will not utilize any facial recognition software in any of its video surveillance that it may implement.

Procedures

1. CCTV Installation and Placement

The Executive Director has the responsibility to authorize all CCTV and web camera surveillance for safety and security purposes at the Museum. All new installations will follow this policy. In carrying out this responsibility, the Committee will also accept input and recommendations from employees of the Museum on suggested camera locations.

2. Notice of Surveillance

Except in applications of forensic video surveillance, signs shall be displayed prominently in public areas covered by video surveillance informing the public of the usage of video surveillance on Museum property.

3. **Notice of Policy**

The Personnel Department shall disseminate this policy among Museum employees. Additionally, this policy shall be posted on the Museum's website.

4. **Placebo Cameras**

The Museum will not utilize inoperative, perfunctory, placebo, or "for looks-only" video surveillance equipment. The existence of placebo cameras lessens the deterrent effect of all video surveillance systems.

5. Installation

The Facilities Department shall oversee the installation of all approved surveillance equipment.

6. **Training**

All personnel involved in the supervision, application, use or monitoring of video surveillance technology will meet the following requirements:

1) Be trained in the technical, legal and ethical parameters of appropriate camera use; and
2) Receive a copy of this policy and provide written acknowledgement that they have read and understood its contents.

Access & Storage

Viewing access to video surveillance monitors will be limited. Specifically, the following guidelines shall apply in granting access to monitor the video surveillance cameras:

1) PPD and IT Management will be permitted access to monitor all cameras at all times.
2) Department heads will be permitted access to monitor all cameras that capture images or areas that fall within their work area or building location.
3) Other staff personnel shall be permitted access to monitor cameras that capture images or areas that fall within their work area or building location only with the written permission of their Department head and the approval of the Police Chief.
4) No other access shall be granted to any member(s) of the public unless otherwise sought and requested under Public Record provisions. The request shall identify the individual for whom access is sought, the area to be monitored, and the rationale for why access should be granted. The decision to grant access will be made by the Police Chief.

Video recordings or other media will be stored and transported in a manner that preserves security. Further, recorded images not related to or used for an investigation shall be kept confidential and destroyed on a regular basis. Accordingly, the following guidelines regarding the storage of video surveillance records shall be strictly adhered to:

1) Location: Video surveillance records shall be stored in a secure location as directed by the IT Department, designed for the storage of video recordings with access limited to authorized personnel only.

2) Timeframe: Generally, video surveillance records shall be stored for a period of not less than **30 days**, after which they will be promptly erased, unless retained as a part of a criminal investigation, court proceedings (criminal and civil) or other bona fide use, as approved by the Police Chief. However, the Police Chief may determine that video surveillance records of identified high priority areas be stored for a period of not less than 90 days before being erased.
3) Alterations: No attempt shall be made to alter any part of any surveillance recording. Surveillance centers will be configured so as to prevent camera operators from tampering with or duplicating recorded information.

4) Access Log: An access log shall be maintained by the Information Technology Department of all instances of access to, or use of, surveillance records. This log shall include the date, time, and identification of the person or persons to whom access was granted, as well as a summary of the reason for which access was necessary.

Public records requests

All public records requests, including requests for the release of video surveillance footage, should follow the procedures outlined by Massachusetts Public Record Law.