	Campus Camera Surveillance Policy and Procedure
Domain:	Introduction
Effective Date:	5/9/2025
Date(s) of Revision:	5/9/2025

PURPOSE AND SCOPE

This policy and procedure establishes guidelines for the use, access, and management of surveillance cameras on campus, with specific emphasis on protecting privacy in residential cottages while maintaining security protocols across campus facilities. Security cameras are installed to enhance the safety and security of the MHCO campus. The Security Resource Officer is responsible for monitoring and managing the security camera system in accordance with this policy.

ACCESS PERMISSIONS

Only authorized personnel will be permitted access to cameras governed by this policy. MHCO's Administrator is permitted absolute access to all campus camera footage. MHCO's Security Resource Officer and Program Director are to have access to all campus camera footage excluding indoor residential cottage feeds. The Chief Finance Officer is permitted to have access to the Cobb Center lobby camera feed and Cobb Center doorbell camera feed. The Community Support Coordinator is to have permitted access to the Community Support Center doorbell camera feed. SGA Manager, Office Manager, and Production Manager are to have permitted access to SGA doorbell and back dock camera feed. The Security Resource Officer is to monitor security camera feeds on a regular basis to ensure the safety and security of the campus. In the event of an incident requiring review of indoor cottage camera footage, the Administrator or MHCO's IT vendor, TenPlus Systems, are permitted access to review and export footage directly related to the specific day, time, and location of incident. Tickets submitted to TenPlus for footage retrieval should be sent via email to priorityservice@tenplus.com and must include the specific day, time, and location of the incident. Incident footage should then be provided to MHCO's Administrator, Security Resource Officer, and Program Director for review and documentation as appropriate.

PRIVACY AND CONFIDENTIALITY

All footage is considered confidential information. Footage may not be shared, copied, or distributed without explicit authorization from the Adminstrator. Viewing of footage is restricted to the purposes outlined in this policy and should only occur when there is a legitimate reason for doing so including but not limited to safety concerns, licensing, criminal investigation, or legal requests.

COMPLIANCE

All specified users must comply with this policy. Logs of footage review will be accessed monthly by the Security Resource Officer. Specified users shall sign an acknowledgement of and agree to this policy yearly and when policy changes occur. If any of the directives are violated or if actions are deemed as misuse or misconduct relating to MHCO's Campus Camera Surveillance System, network connections, or computer equipment the individual may be subject to suspension from use of the system for a period of thirty (30) days, sixty (60) days, ninety (90) days, indefinitely, or other disciplinary action including termination of employment, or legal action including personal liability under civil and criminal law. Unauthorized access to camera feeds or improper use of surveillance footage may result in disciplinary action up to and including termination of employment.

RECORDING AND STORAGE

Security Camera footage will be recorded and stored for a minimum of 30 days. Recorded footage will be stored in a secure location both on and off-site and will only be accessible to authorized personnel as outlined within this policy.

MAINTENANCE

The Security Resource Officer will ensure that all security cameras are maintained and repaired as needed to ensure proper functioning. Regular visual inspections will be conducted to identify and address any issues with the security camera system. Should maintenance be required a ticket must be submitted to TenPlus Systems within twenty-four hours of discovering the problem. When reporting problems or making a request for additional computer services at MHCO employees must submit a detailed email to TenPlus Systems at priorityservice@tenplus.com with a carbon copy to the IT Point of Contact or by dialing 919-832-5799 and choosing option #3 for the help desk at TenPlus Systems. The IT Point of Contact shall follow up via visit, phone call, or email within ten (10) business days of determining the problem was corrected.