Security Systems Policy

Purpose and Principles

The purpose of this policy is to regulate the use of security systems on Champaign County, Illinois property, which include, various ID Badges, Door Access Systems, and Camera Systems throughout multiple County-owned and operated buildings and digital communications and other electronically stored information on software or hardware purchased by the County.

The principles of this policy:

1. Enhance the health and safety of the County personnel, non-County personnel, vendors, contractors, and visiting public; as well as protect County property.
2. Respect the privacy of staff members, public members, and guests.
3. Provide transparency in the use of video camera technology, digital communication platforms, and other security reporting systems in achieving a safe and secure Champaign County campus environments.

Security cameras, access control systems, and digital communications platforms will be used in a professional and ethical manner in accordance with Champaign County policy and local, state, and federal laws and regulations.

This policy does not apply to any County-owned and operated detention facilities.

Definitions

As used within this policy, the following terms are defined as follows.

Audit Log

A chronological record of actions and events within a system, often used in door control systems to track access. It provides a detailed history of who entered or exited a facility and when, which helps with security, compliance, and investigations.

County Executive

Refers to the elected position of Champaign County Executive or their designee. The County Executive is responsible for implementing and managing this policy in all County buildings except the Courthouse and detention facilities.

County Sheriff

Refers to the elected position of Champaign County Sheriff or their designee. The County Sheriff is responsible for implementing and managing this policy in the Champaign County Courthouse.

Detention Facility

Is a place where individuals are held temporarily for reasons like pending court appearances, proceedings, or serving short-term sentences. It's distinct from a prison, which is for long-term incarceration after conviction. Detention facilities can include jails, holding facilities, and juvenile detention centers.

Also Known As: Jail, JDC, Courthouse Cell, Cells

Digital Communication Platform

All software and hardware purchased by the County that allows for digital communication, such as email, instant messaging, and call logs.

Door Access System

A security system that regulates who can enter and exit a building or specific areas within it, using electronic methods to manage access. It replaces traditional key systems with digital solutions like cards, keypads, or biometric scanner.

Also Known As: Door Control, Door Control System, Door Access Control

Hardware

The machines, wiring, and other physical components of a computer or other electronic system.

ID Badge

A physical card or piece of plastic worn by an individual to identify them as a member of a particular organization, division, department, group, or workplace. It typically includes basic information like the person's name, photo, and sometimes their job title, personal descriptors, and department.

Also Known As: Identification Badge, Badge, Card, ID, Prox, Swipe Card.

ID Badge System

Combines software, data, and a printer to create and manage identification badges. A printer in this system is specifically designed to print high-quality, durable identification cards, often made of PVC plastic, with custom designs, images, barcodes, and security

features. These systems are used for various applications like employee badges, student IDs, membership cards, and access control cards.

Key Pad

A keyless access control system that lets you control who can and cannot enter a building or room. To use a keypad door entry system, tenants punch in a numeric code instead of using a physical key.

Electronic/Proxy Card

A contactless smart card that uses Radio Frequency Identification (RFID) technology to allow access to a building or area by being held near a reader, rather than inserted or swiped.

Also Known As: Prox Card, Key Card, “FOB”, Badge, ID

Proximity Reader

A device that reads information from a contactless smart card (or "proximity card") without requiring physical contact, allowing authorized users to gain access to a controlled area.

Also Known As: Prox Reader, Badge Tap, Badge Reader, ID Reader

Security camera

A camera used for monitoring or recording public areas for the purposes of enhancing public safety, monitoring restricted areas or equipment, to discourage theft and other criminal activities, and for preventing, investigating, and resolving incidents. The most common security cameras rely on closed circuit television or network connection using IP.

Security camera monitoring

The real-time review or watching of security camera feeds.

Security camera recording

A digital or analog recording of the feed from a security camera.

Security camera systems

Any electronic service, software, or hardware directly supporting or deploying a security camera.

Software

The programs and other operating information used by a computer

ID Badges – Policy

Responsibilities and Authority

Responsibility for oversight of security cameras and associated policies, standards, and procedures, is delegated by the County Executive and the County Sheriff. This responsibility includes:

1. ID Badge Design and Layout
2. ID Printing
3. Creation, maintenance, and review of a county strategy for the procurement, deployment, and use of ID Badges, including this and related policies
4. Designation of the standard county ID Badge system or service

ID Badge Policies

1. ID Ownership

1. Employees are responsible for the safe keeping and correct use of their assigned ID.
2. IDs are distributed by the County Executive's Office and the Sheriff's Office in applicable circumstances.
3. This ID is not to be duplicated or destroyed.

2. Borrowing / Lending

1. Borrowing and lending IDs is strictly prohibited. Specific IDs are created by HR for general use in the event a temporary employee, visitor or card owner forgets their ID and needs temporary access to the building. IDs are not to be lent or borrowed between card users.
2. If an employee is found to be lending their ID, disciplinary action may be taken.

{END OF ID Badges – POLICY}

Door Access System – Policy

Responsibilities and Authority

Responsibility for oversight of Door Access System and associated policies, standards, and procedures, is delegated by the County Executive and the County Sheriff. This responsibility includes:

1. Creation, maintenance, and review of a county strategy for the procurement, deployment, and use of door access systems, including this and related policies
2. Designation of the standard county door access system or service
3. Review of Audit Log shall be used for troubleshooting and testing of the system, or for the purpose of findings in an investigation only. Unless given direct written authority by the County Executive or County Sheriff, no other user may review the system's Audit Log. Current management is by Human Resources and Facilities as delegated to by the County Executive.

Control Elements

1. Door Access Placement

1. The County Executive and the County Sheriff may establish placement of door access in county owned buildings.
2. Approval from the County Executive or the County Sheriff to install any door access in a county owned building is required.
3. Failure to comply with this policy will result in the department/unit covering the cost to remove and repair the area of installation. The County Executive and the County Sheriff reserve the right to remove all door access deemed to not comply with this policy.

2. Door Access Monitoring

1. The County Executive and the County Sheriff or their assigned staff; may monitor and review door access logs as needed to support investigations and to enhance public safety.
2. Unless approved to review by the County Executive or the County Sheriff through the formal investigative request process, no other staff member or member of the public may view the door access logs.

3. Door Access Retention

1. Door access logs will be retained for a period of no less than 30 and no longer than 120 days. This retention period may be extended at the request of County legal counsel, the County Executive, the County Sheriff, or as required by law.
2. Incident records will be retained, beyond the above retention schedule, for the duration of any relevant investigation. Thereafter the recording will be destroyed. If deemed necessary to retain indefinitely, a formal request must be submitted and approved to the County Executive or the County Sheriff.

3. Retention of door access logs are subject to the requirements of the Local Records Retention Act and the County Executive and County Sheriff are responsible for their respective buildings.

{END OF DOOR ACCESS – POLICY}

Camera – Policy

Responsibilities and Authority

Responsibility for oversight of security cameras and associated policies, standards, and procedures, is delegated by the County Executive and the County Sheriff. This responsibility includes:

1. Creation, maintenance, and review of a county strategy for the procurement, deployment, and use of security cameras, including this and related policies
2. Designation of the standard county security camera system or service
3. Authorizing the placement of all security cameras
4. Authorizing the purchase of any new security camera systems
5. Reviewing existing security camera systems and installations and describing required changes to bring them into compliance with this policy
6. Creating and approving county standards for security cameras and their use
7. Creating and approving the procedures for the use of security cameras

Control Elements

8. Security Camera Placement

1. The County Executive and the County Sheriff may establish temporary or permanent security cameras in public areas of the county.
2. Audio recordings are prohibited.
3. Security cameras may not be used in private areas of County facilities, pursuant to state civil and criminal law.
4. Private areas include: bathrooms, shower areas, locker and changing rooms, areas where a reasonable person might change clothes, and private offices. Additionally, rooms for medical, physical, or mental therapy or treatment are private. Where security cameras are permitted in private areas, they will to the maximum extent

possible be used narrowly to protect money, real or personal property, documents, supplies, equipment, or pharmaceuticals from theft, destruction, or tampering.

5. To the maximum extent possible security cameras shall not be used to get close-up video through the windows of any private residential space or office. If needed, electronic shielding will be placed in the security camera so that the security camera cannot be used to look into or through windows.
6. To the maximum extent possible, security cameras shall not be directed at the windows of any private building not on Champaign County property.
7. Approval from the County Executive or the County Sheriff to install any camera in a county owned building is required.
8. Failure to comply with this policy will result in the department/unit covering the cost to remove and repair the area of installation. The County Executive and the County Sheriff reserve the right to remove all cameras deemed to not comply with this policy.
9. Security Camera Monitoring and Review

1. Review of Security Camera Recordings

1. The County Executive and the County Sheriff or their assigned staff; may monitor and review security camera feeds and recordings as needed to support investigations and to enhance public safety.
2. Unless approved to review by the County Executive or the County Sheriff through the formal investigative request process, no other staff member or member of the public may view the camera system's footage or recordings.

2. Monitoring of Security Camera Feeds

1. Monitoring individuals based on characteristics of race, gender, ethnicity, sexual orientation, disability, or other protected classification is prohibited.

10. Notification Requirements

1. All locations with security cameras will have signs displayed that provide reasonable notification of the presence of security cameras. At a minimum this must include primary building entrances. All proposals for the deployment of security cameras will include proposed sites for the placement of notifying signs. The placement of the signs and the text on the signs will be subject to the review and approval of the County Executive and the County Sheriff.

11. Use of Recordings

1. Security camera recordings, with the approval of the County Executive or the County Sheriff, are to be used for the purposes described in the definition of a security camera. This use extends to their release by the County Executive and the County Sheriff to external law enforcement agencies. Records of the access to, and release of, security camera recordings must be sufficient so as to validate compliance with this policy.

12. Retention of Security Camera Recordings

1. Security camera recordings will be retained for a period of no less than 30 and no longer than 120 days. This retention period may be extended at the request of County legal counsel, the County Executive, the County Sheriff, or as required by law.
2. Incident records will be retained, beyond the above retention schedule, for the duration of any relevant investigation. Thereafter the recording will be destroyed. If deemed necessary to retain indefinitely, a formal request must be submitted and approved to the County Executive or the County Sheriff.
3. Retention of security camera recordings are subject to the requirements of the Local Records Retention Act and the County Executive and County Sheriff are responsible for their respective buildings.

{END OF CAMERA – POLICY}

Digital Communication – Policy

Responsibility and Authority

Responsibility for oversight of digital communications and associated policies, standards, and procedures, is delegated by the County Executive. Digital communications include but are not limited to emails, instant messages, and call logs on County-owned hardware or software.

This responsibility includes:

1. Creation, maintenance, and review of a county strategy for the procurement, deployment, and use of digital communication platforms, including this and related policies
2. Implementation and management of secure data protection, including encryption, appropriate restrictions, and password management

3. Implementation and management of digital record keeping in accordance with the Local Records Retention Act
4. Authorizing the purchase of any new digital communication systems
5. Creating and approving county standards for access and account management in all digital communication platforms
6. Ensuring the annual state required cybersecurity training is provided to employees

Control Elements

1. Privacy

1. Employee communications conducted on County-issued devices or utilizing County communication systems are considered the property of the County.

2. Security

1. The County Executive may implement password strength requirements and two-factor authentication.
2. The County Executive may authorize the use of testing of phishing and may require training of employees.

3. Use of Digital Communication Records

1. Digital Communications Records, with the approval of the County Executive, are to be used for the purposes described in the definition of digital communications. This use extends to their release by the County Executive to external law enforcement agencies. Records of the access to, and release of, Digital Communications Records must be sufficient so as to validate compliance with this policy.

4. Retention of Digital Communication Records

1. Incident records will be retained, beyond the above retention schedule, for the duration of any relevant investigation. Thereafter the recording will be destroyed. If deemed necessary to retain indefinitely, a formal request must be submitted and approved to the County Executive.
2. Retention of digital communication records are subject to the requirements of the Local Records Retention Act and the County Executive is responsible for managing or delegating appropriate retention and destruction.

{END OF DIGITAL COMMUNICATIONS – POLICY}

Use of Security System and/or Digital Communications in HR Issues

In the event a department head wishes to review any form of security or digital communication record for the purposes of investigating an employee regarding their work performance, work quality, or potential violation of the law, a formal request must be made through a Security Review Request form and submitted to the HR Manager for review and determination. Initiating a formal review of security and/or digital communication records for the purposes of an HR investigation will be handled in a formal manner according to applicable policy or collective bargaining agreement.

Public Safety Concern

In the event there is an eminent and credible concern for public safety in a County-owned building, the County Executive and County Sheriff may suspend this policy to ensure the safety of County employees and the public in the building are not delayed or denied.

Compliance

The County Executive and the County Sheriff will ensure that records related to the use of security cameras and recordings from security cameras and digital communication records are sufficient to validate compliance with this policy. Units that maintain or support security camera technology and digital communications must also maintain records and configure systems to ensure compliance with this policy. Security camera systems procured by units will need to ensure compatibility with the system identified as the county standard set forth by this policy and other polices by the County Executive and the County Sheriff.

A failure to meet the requirements of this policy may result in loss of the privilege to support, maintain, or deploy security cameras at the discretion of the County Executive and the County Sheriff.

Exceptions

As noted above, uses beyond those described in this digital security record policy shall be governed by applicable County policies and laws, which provide a separate process governing use such as for uses required by law or by authorized administrative approval as detailed therein.

Employee Acknowledgment – Security Systems Policy

The full policy is available at –
https://www.co.champaign.il.us/Policies/SecuritySystemPolicy.pdf

ID Badge Policies

1. ID Ownership

1. Employees are responsible for the safe keeping and correct use of their assigned ID.

2. IDs are distributed by the County Executive's Office and the Sheriff's Office in applicable circumstances.

3. This ID is not to be duplicated or destroyed.

2. Lost or Stolen

1. If an employee's ID is lost or stolen, they should report it immediately to HR by emailing hr@champaigncountyil.gov. HR will take the necessary steps to deactivate and replace the ID. A charge of $25 will be deducted from the employee's next paycheck.

3. Borrowing / Lending

1. Borrowing and lending IDs is strictly prohibited. Specific IDs are created by HR for general use in the event a temporary employee, visitor or card owner forgets their ID and needs temporary access to the building. IDs are not to be lent or borrowed between card users.

2. If an employee is found to be lending their ID, disciplinary action may be taken.

Security Camera Placement

1. The County Executive and the County Sheriff may establish temporary or permanent security cameras in public areas of the county.

2. Audio recordings are prohibited.

3. Security cameras may not be used in private areas of County facilities, pursuant to state civil and criminal law.

4. Private areas include bathrooms, shower areas, locker and changing rooms, areas where a reasonable person might change clothes, and private offices. Additionally, rooms for medical, physical, or mental therapy or treatment are private. Where security cameras are permitted in private areas, they will to the maximum extent

possible be used narrowly to protect money, real or personal property, documents, supplies, equipment, or pharmaceuticals from theft, destruction, or tampering.

5. To the maximum extent possible security cameras shall not be used to get close-up video through the windows of any private residential space or office. If needed, electronic shielding will be placed in the security camera so that the security camera cannot be used to look into or through windows.
6. To the maximum extent possible, security cameras shall not be directed at the windows of any private building not on Champaign County property.
7. Approval from the County Executive or the County Sheriff to install any camera in a county owned building is required.
8. Failure to comply with this policy will result in the department/unit covering the cost to remove and repair the area of installation. The County Executive and the County Sheriff reserve the right to remove all cameras deemed to not comply with this policy.

Digital Communication Security and Privacy

5. Privacy

1. Employee communications conducted on County-issued devices or utilizing County communication systems are considered the property of the County.

6. Security

1. The County Executive may implement password strength requirements and two-factor authentication.
2. The County Executive may authorize the use of testing of phishing and may require training of employees.

By signing below, I acknowledge that I have read and understood the portions of the Champaign County Security Systems Policy that include employee responsibilities and ramifications.

Print Employee Name: _____

_____ _____

Employee Signature Date