# OFFICE OF INSPECTOR GENERAL

## Clerk of the Circuit Court and County Comptroller
## St. Johns County, Florida

# AUDIT REPORT
## Audit # FY25-AP001
## St. Johns County Facilities Management

Brooke Tefft

**Brooke Tefft**
**Inspector General**

August 17, 2026

**Date Issued**

**Brandon J. Patty**
Clerk of the Circuit Court
and County Comptroller

**Brooke Tefft**
Inspector General

# Office of Inspector General

Clerk of the Circuit Court & County Comptroller
St. Johns County, Florida

August 17, 2026

The Honorable Chairman and Members of the Board of County Commissioners

The Office of Inspector General has concluded an audit of procedures regarding life safety and access control systems within the Facilities Management Department.

We wish to formally acknowledge and extend our sincere appreciation to the staff of the Facilities Management and County Administration Departments for their exemplary cooperation and assistance throughout the course of this audit engagement.

This audit was performed in accordance with the Global Internal Audit Standards of the Institute of Internal Auditors (IIA) and the Principles and Standards for Offices of Inspector General established by the Association of Inspectors General (AIG).

We believe that the recommendations in this report will support the St. Johns County Board of County Commissioners in its continued commitment to delivering reliable, effective, and efficient services to residents while maintaining the highest standards of governance and compliance with all applicable laws and regulations.

Respectfully,

Brooke Tefft

Brooke Tefft, CFE, CCEP & CTTO
Inspector General

cc:
Brandon J. Patty, Clerk of the Circuit Court and County Comptroller
Joy Andrews, County Administrator
Brad Bradley, Deputy County Administrator
Jesse Dunn, Deputy County Administrator
Dan Whitcraft, Facilities Management Director

# Table of Contents

# I. EXECUTIVE SUMMARY

This audit assessed the presence and effectiveness of access controls for physical keys and employee identification badges, both overseen by the Facilities Management Department for St. Johns County. The audit findings indicate that policies, procedures, and internal controls for physical keys are inadequate. Whereas those for badge access are generally satisfactory, apart from the observations documented in the report.

The audit identified 10 findings, each accompanied by specific recommendations to ensure accurate tracking and optimal resource utilization, ultimately supporting Facilities Management's mission to ensure the security and safety of all St. Johns County employees and visitors to the St. Johns County buildings. Findings related to key access include a lack of policies and procedures, insufficient documentation of issued and circulating keys, a highly variable key inventory, and the absence of criteria for key issuance. Findings related to badge access include a lack of documentation to support badge changes, decentralized badge management, and insufficient policies and procedures.

# II. PURPOSE

Based on the 2025 County-wide Risk Assessment, the Office of Inspector General (OIG) 2025 Annual Audit Plan included an audit of procedures for life safety and access control systems within the Facilities Management Department.

# III. BACKGROUND

The St. Johns County Facilities Management (SJCFM) Department consists of three divisions: Building Operations, Facilities Maintenance, and the Sheriff Complex Maintenance Division. The goal of SJCFM is to provide an attractive, clean, and safe environment for all users of County facilities in a cost-effective manner.

The Building Operations (SJCBO) Division has 19 employees working in seven locations throughout the county. They are responsible for the property management of the Judicial Campus and Annex locations, and manage:

- Access control systems.
- The Central Receiving Mail Program.
- Janitorial and facility maintenance services.

As a part of the access control systems, SJCFM is responsible for managing the creation of physical keys, the activation/termination/access levels for employee identification badges, and maintaining the badge systems for the Board of County Commissioners, St. Johns County Clerk of the Circuit Court and County Comptroller (COCC), County Attorney, St. Johns County Supervisor of Elections (SOE), St. Johns County Tax Collector (Tax Collector), St. Johns County Property Appraiser, and State Attorney.

**<u>Physical Keys</u>**

SJCFM manages the inventory of physical keys and processes key requests and related work orders. The types of physical keys for the Judicial Campus and Annexes are detailed in Table 1. Tracking of Enhanced Security Area Master keys/Assigned keys, Sub Master keys, and Change (standard office door) keys is the responsibility of individual departments/agencies.

**Table 1**

| **Type** | **Access Provided** | **Holders** | **Inventory Maintained by Bldg. Ops.** |
|---|---|---|---|
| **Control** | Does not provide ingress/egress, but is required for all lock modifications | • BO Superintendent<br>• BO Property Manager<br>• BO Maintenance Technician III<br>• BO Maintenance Technician II | Yes |
| **Great Grand Master (GGM)** | Exterior and Interior Doors, except enhanced security areas within the Judicial/Administrative Complex | • SJCBO Superintendent<br>• SJCBO Property Manager<br>• SJCBO Maintenance Technicians<br>• Custodians<br>• Courthouse Bailiffs<br>• County Administration Executives<br>• | Yes |
| **Enhanced Security Area – Master Key** | All door locks in an enhanced security area | • Supervisor(s) of the enhanced security area | No |
| **Enhanced Security Area - Assigned** | Assigned lock(s) in an enhanced security area | • Supervisor(s) of the enhanced security area<br>• Employee Assigned | No |
| **Sub Master** | Opens all doors within one suite | • Department Directors<br>• Supervisors<br>• Designated Key Custodian staff | No |
| **Change (Standard Door)** | Employee Office Door | • Employee Supervisor<br>• Employee | No |
| **Other** | Padlocks, storage sheds, mechanical rooms, etc. | • SJCBO Superintendent<br>• SJCBO Property Manager<br>• Assigned Employees | Yes |

The creation of keys, including replacements and new requests, is outsourced to a third-party vendor. SJCFM manages this contract. Once a new key is produced, it is documented and secured in a lockbox. If a key is lost or broken, SJCFM is notified to arrange for a replacement. Before issuing a key, a Receipt of Key form (Appendix A) must be completed.

SJCFM uses MicroMain to capture all requests for lock malfunctions.

**ID Badges**

SJCFM issues badges to employees of the Board of County Commissioners (BOCC), as well as to other elected officials and agencies housed in county-maintained buildings, contracted workers, and visitors upon request. The BOCC HR creates the physical badge, which includes the badge holder's information and photograph. SJCFM then assigns security parameters to each badge based on a completed Request For St. Johns County Badge form (Appendix B).

For BOCC staff, SJCFM personnel receive notifications of employee hires, transfers, and discharges through NeoGov, the County's Human Resources system. Related forms and documentation are stored in this system. For non-BOCC staff, SJCFM personnel receive emails and/or phone calls about updates to employee status, as well as SCJ Badge Form submittals, which result in badge issuance, updates, or deactivation/deletion.

The Apollo APACS system is used to create, modify, and deactivate/delete employee badges. The system allows SJCFM staff to set access hours and specify which doors or areas are accessible. It has the capability to track when badge changes are made, as well as the time and location when badges are scanned to enter secure areas.

The MicroMain system is used to input, document, and complete work orders. This includes an automated task generated every Monday to check the status of all access control panels, readers, and cameras. If a reader has an issue, a work order is created to repair it. Work orders are also generated in the MicroMain system when a call or email is received, alerting staff to a badge reader issue.

## IV. OBJECTIVE, SCOPE, AND METHODOLOGY

**The objectives of the audit were:**

- To evaluate the presence and efficacy of policies and procedures used to track access to physical keys, authorized issuance of physical keys, and disbursement and disposition of physical keys
- To evaluate the presence and efficacy of internal controls in place that ensure badge access is authorized correctly, and changes to access are implemented in a timely manner
- To evaluate the presence and efficacy of policies and procedures implemented to ensure the proper functioning of badge readers.

**The scope of this audit** encompassed access controls managed by SJCFM. The period under review was October 1, 2023, through September 30, 2024. The scope was modified for the review of badge changes to cover the period from September 1, 2024, through December 31, 2024. This change was made to avoid capturing data before the implementation of unique user access for all changes within the badge system. Prior to this change, all users used the same access ID.

**The audit methodology included**, but was not limited to:

- Interviews with appropriate staff
- Review of policies, procedures, and related requirements
- Completion of process walk-throughs
- Review of records and reports
- Review of user permissions
- Review of work orders
- Detailed testing of selected transactions

## V. STATEMENT OF AUDITING STANDARDS

This audit was conducted in accordance with the Global Internal Audit Standards and with the Principles and Standards for Offices of Inspector General. Those standards require that the OIG plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on the audit objectives. Findings are prioritized based on significance in accordance with Standard 14.3. The OIG believes the evidence obtained provides a reasonable basis for our findings and conclusions based on the audit objectives.

## VI. FINDINGS AND RECOMMENDATIONS

►► **Finding #1: There are no written procedures related to keys and key controls.**

There are no documented procedures regarding physical keys. Additionally, there are no written criteria to establish when a key should be issued. The existing process involves a Superintendent review of access levels. The current staff is in the process of developing appropriate procedures. Tracking of Enhanced Security Area Master keys/Assigned keys, Sub Master keys, and Change (standard office door) keys is the responsibility of individual departments/agencies.

Documented procedures ensure uniform application of practices across the organization. Furthermore, they facilitate continuity of services in the event of employee departure by providing a clear operational roadmap.

A lack of written procedures can lead to improper documentation, failure to implement controls, or risk of loss or damage to county assets.

| | |
|---|---|
| **Recommendations**: | • SJCFM continues to create procedures for all operational functions.<br>• Management establishes written criteria for the issuance of keys. |
| **Management Responses**: | See Appendix D |

**►► Finding #2: The total known number of physical keys issued by SJCFM in current circulation is unidentifiable.**

There is no complete record of all physical keys issued, in circulation, or returned. This includes all keys listed in Table 1.

Over the past two years, SJCFM has tracked the number of keys issued following the implementation of the "Receipt for Key" form (see Appendix A). Prior to this new procedure, there was no record of issued keys, including new requests or replacements. The "Receipt for Key" form provides a hard-copy record of issued physical keys but does not document their return and is not stored electronically or in a manner accessible to all authorized parties. The form applies only to physical keys tracked by SJCFM; tracking of Enhanced Security Area Master keys/Assigned keys, Sub Master keys, and Change (standard office door) keys is the responsibility of individual departments/agencies.

SJCFM does not have written internal-use procedures or procedures for departments and agencies that manage their own keys.

Due to the lack of centralized key management, there is no verifiable record of all keys, keyholders, and individuals with access to them. Many of the agencies to which SJCFM issues keys handle highly sensitive data and could pose safety risks if that information were exposed.

| | |
|---|---|
| **Recommendations**: | • SJCFM develops a process for centralized management of all physical keys issued, including those for office doors, GGM, padlocks, special request keys, etc.<br>• Management requires signed documentation of the issuance and return of physical keys.<br>• Management develops a process for centralized storage of signed documentation of physical keys in a manner that allows for access by all appropriate staff.<br>• Management considers changing locks through County-maintained buildings with a prioritization of those with highly sensitive data and high safety risks. |
| **Management Responses**: | See Appendix D |

**►► Finding #3: Documentation to support badge changes is not consistently obtained or centrally stored.**

Based on the review of badge changes and the related policy, procedures, and SOPs, the following forms have been identified for documenting badge modifications, including initial requests, access levels, deactivations, and deletions:

- Request for St. Johns County Badge (see Appendix B)
- St. Johns County Badge Request Form – New Employee (generated by NeoGov)
- Badge Photo Update and Replacement Form (generated by NeoGov)
- Fitness Center & Class Participation Waiver – grants badge access to the employee fitness centers (see Appendix C)
- Separation Personnel Notice (generated by NeoGov)

Email requests for badge changes for BOCC employees, non-BOCC employees, and contractors are sent individually to the Facilities Technology Supervisor and the Administrative Coordinator. Email requests and any related follow-up communication are retained only in the employees' individual email boxes and not saved to a centralized location. The physical forms listed above were stored as hard copies only, electronically scanned, or generated and completed within the NeoGov system.

It was noted that, in addition to SJCFM employees, specified staff from BOCC Human Resources, Fire Rescue, the Tax Collector, and the Supervisor of Elections offices can create and modify badges for their respective areas. These staff are designated in the system as "Operators". SJCFM staff does not process these modifications but can assist with system malfunctions. Fire Rescue, the Tax Collector, and the Supervisor of Elections offices may make changes without SJCFM staff approval and are not required to provide documentation to support badge access changes. The bailiffs and guards do not have access to create badge modifications but have access to alarm mode.

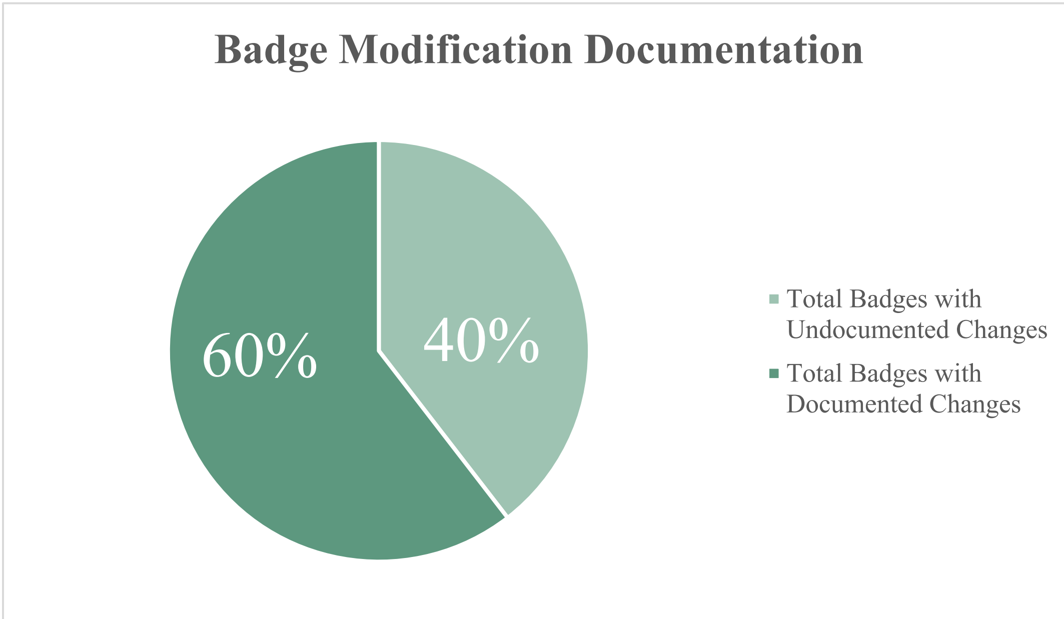
**Badge Modification Sample**

From September 1, 2024, through December 31, 2024, there were changes to 499 badges. Of these, 177 were selected for review. Upon completion of testing, it was determined that 70 distinct badges underwent changes on 85 separate occasions, but these changes were not adequately documented with an email or a corresponding badge form (Table 2). Of these 70 badges lacking appropriate documentation for changes, the following were noted.

- 22 were edited by the SOE.
- 15 were edited by Fire Rescue.
- Nine were for the COCC.
- Three were edited by the Tax Collector.
- One was a BOCC badge change believed by the Facilities Technology Supervisor to have been initiated by a phone call from a project manager.
- 20 were for BOCC, Contractor, and Department of Health employees.

SJCFM staff was unable to provide the documentation for the 40 undocumented changes edited by Fire Rescue, SOE, and the Tax Collector.

**Table 2**



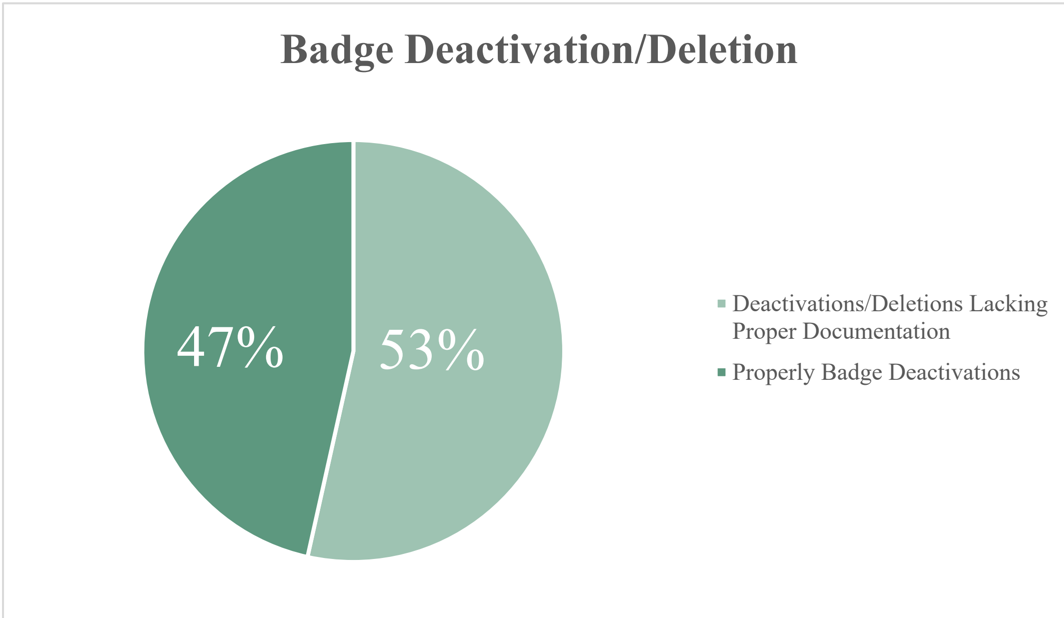

**<u>Badge Deactivation/Deletion Sample</u>**

During the review of badge changes, 43 badge deactivations or deletions were identified. Of these, 23 lacked adequate supporting documentation. Additionally, there is no documentation confirming whether these deactivations or deletions were completed in a timely manner (Table 3). Of these 23 deactivations and deletions, the following were noted.

- Two were edited by Fire Rescue.
- Twelve were edited by SOE.
- Three were deleted on the same day that a different badge was edited for the same badge holder (e.g., an old badge was not deleted).
- One was for a badge that was never physically created. According to the staff, the employee failed to appear.
- Five were for BOCC, Department of Health, and State Attorney badges.

SJCFM staff was unable to provide the documentation for the 40 undocumented changes edited by Fire Rescue, SOE, and the Tax Collector.

**Table 3**




**Review of Documented Changes**

After reviewing the documentation for badge modifications, it was noted that a related request form supported 56 badge access changes, and an email request supported 39. Of those reviewed, the following was noted.

- Three request forms did not indicate access level (daily or 24-hour).
- One request form checked the box for "Other Access" but did not specify the access needed.
- Four request forms were not signed by the badge holder.
- Four request forms did not include the authorizer's signature.
- Ten of the request forms were completed for BOCC employees but were not entered into NeoGov.
- Thirteen of the email requests were BOCC employees and were not completed in NeoGov.

An absence of proper documentation can increase the risk of unauthorized issuance/access of employee badges across various agencies within the county.

| | |
|---|---|
| **Recommendations**: | • SJCFM centrally maintains documentation to support badge creations, changes, deactivations, and deletions.<br>• SJCFM develops a process for ensuring the appropriate staff have access to documentation supporting badge changes. |
| **Management Responses**: | See Appendix D |

**►► Finding #4: The Access Badge Standard Operating Procedure is not adequate to ensure appropriate controls.**

The Access Badge Standard Operating Procedure (SOP) applies to all employee badge functions involving the Human Resources (HR) badge team and the SJCFM badge team. The SOP requires that requests for new-hire badges, badge modifications, and badge deactivations be documented in NeoGov for BOCC employees. For non-BOCC employees and contractors, requests for new-hire badges and badge deactivations must be submitted via email to a designated centralized email address.

The Access Badge Standard Operating Procedures currently omits several vital elements, including:

- It does not require badge change forms for badge deactivations.
- The SOP does not apply to outside agencies or contractors, such as the COCC, Tax Collector, or the SOE.
- Within the process for non-BOCC employees and contractors, there is a lack of supporting information within the emails required for a badge change. The SOP does not specify who can authorize badge changes (e.g., employee supervisor, Human Resources, Department Director, etc.).
- For non-BOCC employees, the SOP does not mandate the return of the deactivated badge to SJCFM for destruction or to provide proof of destruction

| | |
|---|---|
| **Recommendations**: | • SJCFM updates written policies and practices to require:<br>▪ Completion of badge forms for all badge changes and/or sufficient detail in email change requests.<br>▪ Appropriate authorization for badge changes.<br>• SJCFM defines who is an appropriate authorizer for badge changes.<br>• Information recommended for email request documentation includes:<br>▪ Name of badge holder and badge number (if applicable)<br>▪ Department & position of badge holder<br>▪ Date the changes are effective<br>▪ Sign-off of person(s) approving the change<br>▪ Specific changes to be made<br>▪ Purpose of changes (if applicable)<br>• Management establishes a policy that requires the return of badges of terminated employees to SJCFM for destruction or requires proof of destruction of badges.<br>• Management requires all agency HR Teams to send a monthly report of terminations to SJCFM, which is then reconciled with the badge system. |
| **Management Responses**: | See Appendix D |

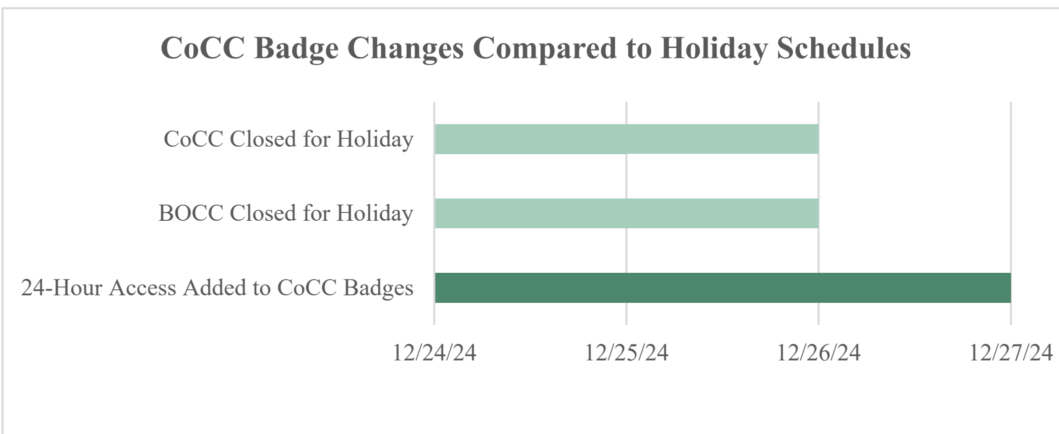
**►►<u>Finding #5: Holiday badge modifications circumvent security protocols and are not appropriately documented.</u>**

The Apollo Badge system provides for two different access types: Daily Access and 24-Hour Access. Daily Access grants badge holders access Monday through Friday from 7:00 am to 6:00 pm, whereas 24-Hour Access provides 24/7 access. Per current policies, supervisor approval is required for obtaining 24-Hour access. BOCC holidays are entered into Apollo by SJCFM, and the system is configured to deactivate badges with daily access during these scheduled BOCC holidays. The system does not support assigning different holiday schedules to individual badges; therefore, all badges, including those assigned to non-BOCC employees, are synchronized with the BOCC holiday schedule.

When an agency, such as the COCC, remains open to the public on a holiday when the BOCC is not operational, SJCFM must manually edit each non-BOCC badge with daily access. To facilitate access during this holiday period, badge holders are granted 24-Hour access. This 24-Hour access will remain in effect until SJCFM staff manually reverts each badge to its previous daily access status.

From September 1, 2024, through December 31, 2024, there were changes to 499 badges. A sample of 177 was selected for review. Of those, nine badges for COCC staff were modified to provide 24-Hour access to accommodate the difference in holidays between the agencies (Table 4).

**Table 4**




Badge change request forms were not completed for employees with temporary badge changes during the holiday. The only documentation supporting the changes is an email from the Facilities Technology Supervisor to SJCFM indicating changes to the badge system to accommodate the holiday schedule. The email suggests that the holiday was removed from the badge system, and readers were subsequently modified for BOCC buildings.

Modifying daily badges to 24-hour access can result in unauthorized access to County assets.

| | |
|---|---|
| **Recommendations**: | • Management considers changes in the system or use of the system to allow for varying holidays for staff of differing agencies.<br>• Management discontinues the practice of overriding system limitations by providing 24-hour access to badge holders who are<br>• authorized for daily access only. |
| **Management Responses**: | See Appendix D |

►► **Finding #6: Badges and keys created for continuous contractors are not tracked, and documentation of contractor badge verification is not retained.**

When a badge request for a specific contractor is received, the SJCFM Superintendent verifies that the BOCC has obtained the following:

- Background check
- Submission of identification
- Existing contract with the county
- Existing purchasing order

The documents acquired and reviewed are not retained, and there is no documentation indicating that this review took place or that it is associated with a badge.

Continuous contractors perform duties on an ongoing basis, such as the vendor responsible for elevator maintenance. Because these vendors do not need daily access, they are not issued badges. Instead, vendor badges and keys are created for their use. These badges are kept at the bailiff stations for pickup when needed. Upon arrival to collect a key and/or badge, the vendor is not required to sign out the items or sign them back in upon return. If a vendor fails to return a badge, they must do so within 24 hours. If it is not returned, the badge is deactivated.

This process presents the following risks.

- Contractors who possess a badge may have unsupervised access to secure locations that may contain sensitive data.
- Improper review of vendor badge documentation may result in granting badge access to individuals with criminal backgrounds who do not meet statutory and/or contractual guidelines.
- It may permit access to individuals who are not under contract with the County, thereby posing an increased risk to the people and assets of St. Johns County.
- If an incident affecting critical functions were to occur, the county may face challenges in addressing the incident promptly and effectively.
- Allow an individual posing as a vendor to gain access to confidential areas through the use of a badge or key.
- If there is turnover at the guard station, new personnel may not be adequately informed about the importance of ensuring that all badges and keys are returned.

| | |
|---|---|
| **Recommendations**: | • Management requires all badges and keys to be logged in and out.<br>• Management ensures badge and key logs include the vendor name, contractor name, and date and time of issuance and return of the badge and/or key.<br>• Management requires all badges and keys to be logged in and out. The log should include the vendor's name and the vendor employee's name who retrieved the badge. The log should also include the date and time of issuance and return of the badge/key. |
| **Management Responses**: | See Appendix D |

►► **Finding #7: Documentation to support the issuance of physical keys is not adequate.**

The audit examined all Request for St. Johns County Badge and/or Key Forms completed during Fiscal Year 2024. This form is no longer in use, and a blank sample could not be retrieved. The form does not specify whether a key was issued, lacks a section for key details such as a biting number or unique identifier, and does not include a section to confirm the return of the key and/or badge. A total of eight request forms were completed, and the following observations were made.

- Five forms not signed by the recipient, acknowledging that the key cannot be duplicated and must be returned upon termination of employment.
- Five forms reflect the SJCBO Superintendent as the authorizer, but do not include his authorizing signature.
- Six of the eight forms do not include department head authorization.
- Physical keys were issued for four of the eight people (two are still currently issued, one has been returned, and it is unknown whether the remaining key has been returned). *

*Based on emails or undocumented personal knowledge of the SJCBO Superintendent.

The audit also examined all Receipt for Key Forms completed in Fiscal Year 2024. A total of 15 request forms were completed. Seven were excluded from testing because they were completed by the COCC's Office of Inspector General staff. The following observations were made for the remaining eight.

- Two included a handwritten note that the key was returned, one key was still in circulation, and it is unknown whether the remaining five keys were returned or still in circulation.
- For the two returned keys, there is no sign-off by the keyholder or SJCFM that the key was returned.
- Seven forms did not have proper supervisor authorization.
- One form included no information except the receiver's signature.
- Four forms did not include an SJCFM signature acknowledging the issuance of a key.

| | |
|---|---|
| **Recommendations**: | • Management modifies forms to include key information and the sign-off of the return of keys.<br>• Management requires all forms to be fully completed before the issuance of keys. |
| **Management Responses**: | See Appendix D |

►► **Finding #8: Work orders were not completed in a timely manner.**

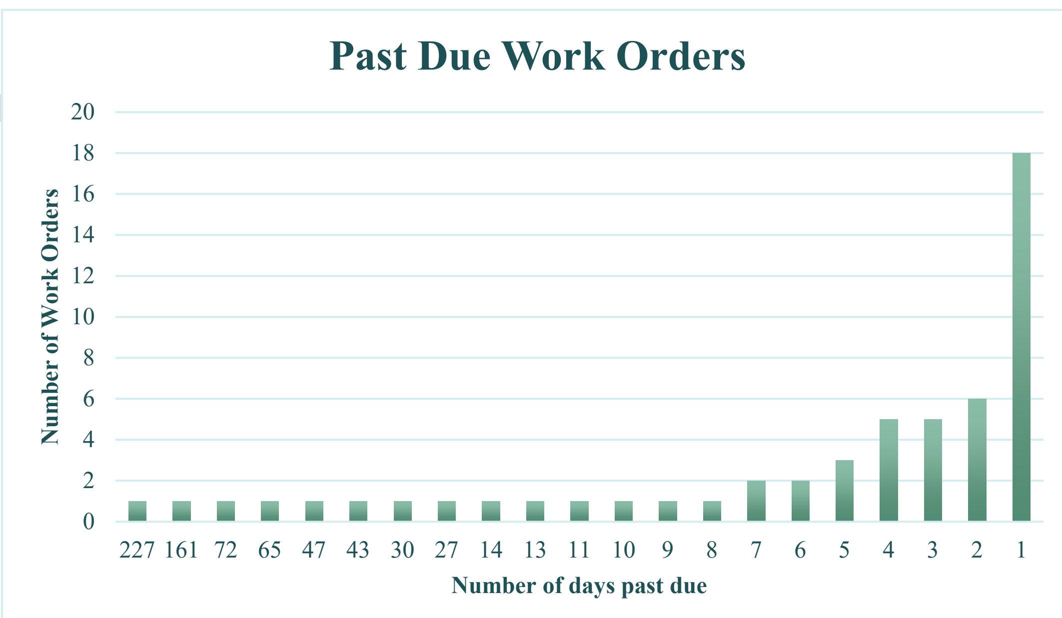
When repairs to county buildings or assets are needed, a work order is created. The requested work is then assessed by designated management, during which it is prioritized and assigned to staff. There are six priority levels that determine the number of days the work must be completed within.

| Priority Level | Days to Complete |
|---|---|
| **1** | 2 |
| **2** | 7 |
| **3** | 14 |
| **4** | 30 |
| **5** | 90 |
| **6** | 365 |

The due date for each work order is determined by the request date and its priority level. The priority level and due date can be adjusted as needed once work commences, based on the anticipated work time estimates.

In fiscal year 2024, 178 work orders related to badge and key requests were completed. Of these, 55 work orders (30.9%) were completed one or more days after their due date. (Table 5)

**Table 5**



The following details were found among the 55 work orders that were completed past due.

- Nine were completed by outside vendors.
- The five most overdue work orders completed in-house involved a lengthy process of ordering parts, consulting vendors, and processing purchase orders.
- Three work orders took seven or more days to issue. These work orders had issue dates 65 days, 13 days, and seven days after the request dates. These delayed issue times led to later past-due completion dates.

Delays in the maintenance and repair of badge and key-related issues could prevent staff from entering or securing assets.

| | |
|---|---|
| **Recommendations**: | • Management develops a process for monitoring past due work orders to determine whether any adjustments are necessary, such as adjustment of priority level, increase of staff or resources delegated to the project, further follow-up, or other necessary actions as needed. Work orders should be updated to reflect adjustments. |
| **Management Responses**: | See Appendix D |

**►► <u>Finding #9: Physical keys issued do not have unique identifiers.</u>**

Physical keys maintained by SJCFM lack a distinctive individual identifier. Some physical keys feature a biting number that signifies the cuts or grooves of the key. However, a biting number does not satisfy the criteria for a unique identifier, as a single biting number may operate multiple locks. When a physical key is issued, and a Receipt for Key form is completed, the physical key does not have a unique identifier that can be documented on the form.

| | |
|---|---|
| **Recommendations**: | • Management ensures all keys issued, particularly those of high-risk areas, include unique identifiers for proper tracking of keys. |
| **Management Responses**: | See Appendix D |

**►► <u>Finding #10: Key inventory is not up to date.</u>**

The Key Box Numerical Index is an inventory of all keys on-site at SJCFM located within the key lockbox. The lock box is used solely to duplicate keys when a new one is needed, and a key does not leave the lock box unless an SJCFM employee takes it to the vendor to create a copy. The inventory is a hard copy that is not maintained electronically. It includes details for 339 keys and the following information.

- File Key Number – Indicates where the key is located within the lock box.
- Location of Lock – Name of Building – Person or Item to Which Key Belongs

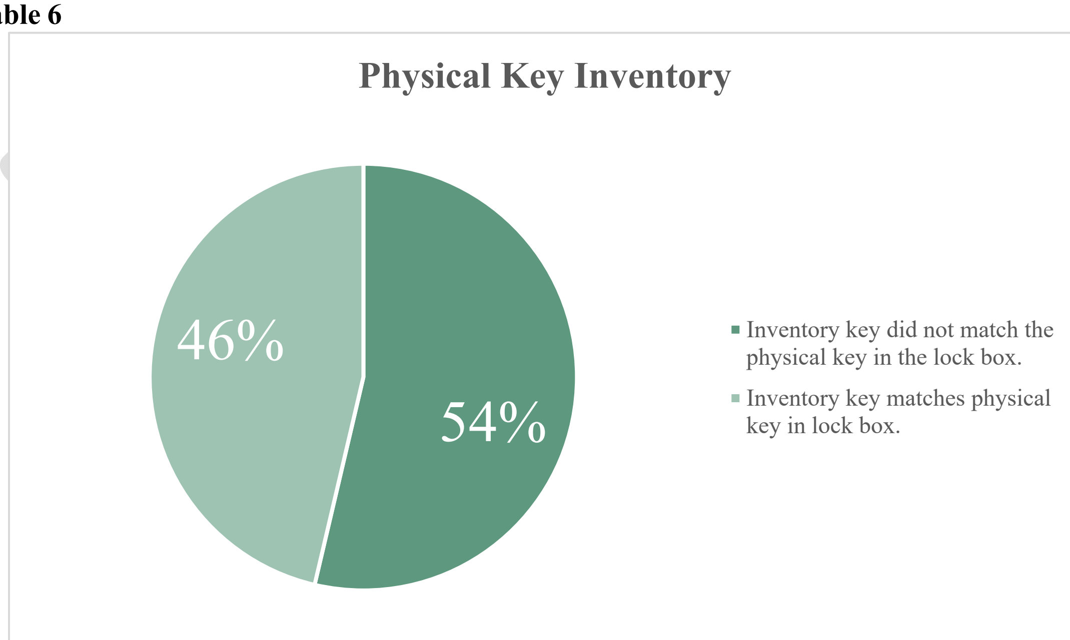
- Keyway & Biting – To identify the key shape and how the key is cut
- If the key is a Master Key or Grand-Master
- Name of Lock Manufacturer and Style of Lock
- Key Code

The key inventory does not include the total number of keys created, the number of keys in circulation, or any information relating to the issuance, return, or destruction of keys. Multiple versions of the inventory were provided. All versions included manual changes, some of which were illegible. The inventories were not dated, and the most current version could not be determined. The inventory used for sampling purposes was titled "Key Box Numerical Index.

A random sample of 181 keys was selected for review. All samples were chosen from the Key Box Numerical Index controlled by SJCFM. No keys tracked by county departments were tested. During testing, the review was discontinued after 41 keys due to inconsistencies. The inventory provided was inconsistent with itself and the keys within the lock box. Out of the 41 keys observed, the following was noted.

- The key listed on the inventory did not match the key in the box for 22 of the keys reviewed. (Table 6)
- Two of the key slots held multiple keys with different biting numbers.
- One key slot that had inventory recorded was empty.
- Four sets of keys did not have biting numbers or any other identifiers etched on them.

**Table 6**



An incomplete or inconsistent inventory creates the risk that, if a key is needed during an emergency, SJCFM staff may not be able to provide it promptly. This could delay access to emergency equipment or other critical resources.

| | |
|---|---|
| **Recommendations**: | • Management develops an electronic inventory that is kept current.<br>• Management ensures all appropriate staff have access to view and edit the key inventory.<br>• Management ensures the inventory includes appropriate data, including the number of keys created, outstanding, and on hand.<br>• Management develops procedures for ensuring outstanding keys are tied to appropriate documentation. |
| **Management Responses**: | See Appendix D |

# Appendix A

# St. Johns County Building Operations
# Receipt for Key

Date: ________________

Name: ____________________

Department:__________________________

Building:________________________ Room #:___________________

Bitting #:________________________

I acknowledge the receipt of the above-mentioned keys. I understand that I am responsible for these keys and will immediately report any theft or loss. I further agree not to have these keys duplicated, and to return them to the Building Operations Superintendent when no longer required for the performance of my duties, or my employment status changes.

__________________________ __________________________
Signature Date

__________________________
Name (please PRINT)

__________________________
Authorized By

# Appendix B

# REQUEST FOR ST. JOHNS COUNTY BADGE

NAME: ______________________________ DATE: __________

JOB TITLE: ______________________________ COUNTY ID#: __________

DEPARTMENT: ______________________________

AUTHORIZED BY: ______________________________

AUTHORIZING SIGNATURE: ______________________________

BADGE TYPE: ◉ COUNTY ○ OTHER ______________________________

BADGE REQUEST TYPE: ◉ INITIAL EMPLOYMENT ○ REPLACEMENT

REASON FOR REPLACEMENT BADGE: ○ LOST ○ TWO YEARS OF WEAR
○ BROKEN ○ CHANGE IN INFORMATION ◉ OTHER ______________

ACCESS LEVEL: ○ DAILY WORK HOURS ○ 24 HOUR ACCESS

**I UNDERSTAND AND AGREE TO THE FOLLOWING:**

- **Unless the damage is work-related, a $10 replacement fee will be charged for any lost or damaged badge while employed payable by check or money order to St. Johns County Board of County Commissioners or via pay check deduction.**
- **I agree that I will not give my County ID and/or my agency ID to any person for his or her use. I also agree to return all County IDs, agency ID, to the Building Operations Manager upon termination of my employment with St. Johns County or the agency from which I received this ID.**

______________________________ ______________

Employee Signature Date

# Appendix C

# **FITNESS CENTER & CLASS PARTICIPATION** WAIVER

Return completed form to bccbenefits@sjcfl.us or fax to 904.209.2414.

**CODE OF CONDUCT**

1. I am using a St. Johns County (SJC) fitness center or participating in a fitness class at my own risk, in a safe manner and during my own unpaid time.
2. I will leave a SJC fitness center or location used for a fitness class in the same condition I found it and report fitness center equipment issues to the Wellness Coordinator.
3. I will not give the entry code for a SJC fitness center to anyone else and I will not open the door for anyone else who does not have the entry code.
4. I will conduct myself in a professional manner and will treat other people and the facility with respect.
5. I will hold myself accountable for violations of this policy and will help enforce the rules.
6. As a St. Johns County employee, I understand spouses, dependents, contractors and other visitors are **not** allowed to use a SJC fitness center or participate in a fitness class.
7. I will follow all posted SJC fitness center rules.

**ASSUMPTION OF RISK, WAIVER & RELEASE OF LIABILITY AGREEMENT**

1. My participation in the St. Johns County Wellness Program is voluntary and is considered to be a recreational and/or social activity which is not a required incident of my employment.
2. I fully understand, acknowledge and accept that my voluntary participation in the St. Johns County Wellness Program is unrelated to my employment.
3. I fully understand and agree that my participation in the St. Johns County Wellness Program must be undertaken by me only during non-working hours. The time I spend exercising is unpaid and is not work time.
4. I fully understand and appreciate the risk of injury from exercise I perform pursuant to the St. Johns County Wellness Program.
5. I knowingly, voluntarily and with fully informed consent do assume all risk of injury, harm, loss, disability or death which may result from any exercise performed through the St. Johns County Wellness Program, including but not limited to the use of equipment and facilities, and participation in any aspect, including but not limited to exercise, diet and/or fitness components, of this program.
6. I, for myself and on behalf of my heirs, assigns, personal representatives, next of kin, and anyone entitled to act on my behalf to recover damages as a result of any injury, harm, loss, claim, disability or death in any way incident to, connected with, or related to my participation in the St. Johns County Wellness and Exercise Program, do hereby waive, release, discharge, hold harmless, and agree to indemnify and defend St. Johns County, Board of County Commissioners of St. Johns County, each of their officers, officials, agents and/or employees, from and against any and all losses, claims, liabilities, causes of action, damages, judgments, costs and expenses of any kind, including but not limited to any worker compensation claims under Chapter 440, Florida Statutes, that arise from, or are in any way incident to, connected with, or related to my participation in any aspect of the St. Johns County Wellness Program.

☐ **I understand this policy and agree to follow all rules whether written, posted or implied.**

☐ **I understand I must sign an Assumption of Risk, Waiver and Release of Liability Agreement for participation in the St. Johns County Wellness Program before being given entry to a SJC fitness center or participating in a fitness class.**

| | |
|---|---|
| Print Name: | Employee ID Number: |
| Department/Division: | |
| Contact Number: | |
| Signature: | Date: |

# Appendix D

July 20, 2026

Brooke Tefft, Inspector General
Office of Inspector General
St. Johns County Clerk of the Circuit Court

Dear Ms. Tefft,

On behalf of St. Johns County, I want to thank you for your operational audit of the St. Johns County Facilities Management Department's access controls (Audit Report FY25-AP001 titled St. Johns County Facilities Management Access Controls). Please consider this letter an official management response to the findings identified by the Office of Inspector General (OIG) of the St. Johns County Clerk of the Circuit Court.

The Facilities Management Department (SJCFM), Human Resources Department, County Administration, and the County's Compliance Officer have reviewed the final draft of the report. We appreciate the OIG audit team's focus on the access control status of the Building Operations Division's physical key inventory and on Facilities Management's role in County-wide programmed ID badge procedures; however, we believe that expanded audit testing, covering all County departments and divisions involved in managing access controls, would have provided the auditors with a comprehensive understanding of the responsibilities and operational processes the County employs to ensure the safety of its facilities. Given the County's various service centers (from jails to libraries to parks to fire stations to administrative facilities), an expanded review is essential to understanding effective controls tailored to each location's specific functions and user needs.

As a result, to facilitate planning for the County's access controls improvements for these two areas, we categorized actionable items into four (4) main categories and included comments on operational processes and staff responsibilities within each, helping readers better understand the context:

- Category I: Physical Key Inventory for Judicial/Admin Campus and Related Procedures
- Category II: Programmed ID Badges and Related Procedures
- Category III: Access to the County Buildings' Secured Areas by Contractors
- Category IV: Work Orders for Control Access Issues

**Plan of Action:**

**I. Physical Key Inventory for Judicial/Administrative Campus and Related Procedures.**

- ✓ Finding #1: There are no written procedures related to keys and key controls.
- ✓ Finding #2: The total known number of physical keys issued by SJCFM in current circulation is unidentifiable.
- ✓ Finding #7: Documentation to support the issuance of physical keys is not adequate.
- ✓ Finding #9: Physical keys issued do not have unique identifiers.
- ✓ Finding #10: Key inventory is not up to date.

The Building Operations Division does not routinely issue physical keys for its area; instead, it stores an inventory of control keys, great-grandmaster (GGM) keys, and submaster keys in a secure location. Building Operations technicians responsible for maintaining the assigned Judicial/Administrative Campus locations receive a GGM key as part of their required tool set. To improve efficiency and increase accountability for this division, staff proposes the following actions:

| Actionable Item | Target Time | Responsible staff | Finding # |
|---|---|---|---|
| Assess the advantages of the electronic key management system currently used by another County location for potential implementation at the Judicial/ Administrative Campus for technicians' use. | Completed. The electronic key management system will be implemented for technicians' use. | Facilities Management Department | 2, 7, 10 |

| Actionable Item | Target Time | Responsible staff | Finding # |
|---|---|---|---|
| Redesign the physical key use procedures to incorporate the electronic key management system for technicians. | During FY 2025-2026: complete by 10/1/2026 | Facilities Management Department, Building Operations Division | 1, 2, 7, 10 |
| Categorize physical keys securely stored by Building Operations into three types—control keys, GGM keys, and submaster keys. Update the inventory records to ensure a unique identifier is assigned to each key. | During FY 2025-2026: complete by 10/1/2026 | Building Operations Division | 9, 10 |
| Consolidate all procedures into a single manual to give Building Operations Division staff clear SOPs for operations and training. | In progress: to be completed by 10/1/2026 | Facilities Management Department, Building Operations Division | 1, 7 |

**II. Programmed ID Badges and Related Procedures.**

- ✓ Finding #3: Documentation to support badge changes is not consistently obtained or centrally stored.
- ✓ Finding #4: The Access Badge Standard Operating Procedure is not adequate to ensure appropriate controls.
- ✓ Finding #5: Holiday badge modifications circumvent security protocols and are not appropriately documented.

The OIG reviewed processes and data from FY 2024, from which they have formulated their recommendations. Beginning in January 2026, the County discontinued services with our previous system provider (NeoGov) as part of our Workday ERP system implementation; as such, County staff proposes the following steps to meet current operational needs for access controls related to programmed ID badges:

| Actionable Item | Target Time | Responsible staff | Finding # |
|---|---|---|---|
| Evaluate business processes and workflows available for configuration in the Workday ERP system to establish authorization procedures for issuing and/or modifying programmed ID badges and storing supporting documentation if necessary. | In progress, pending Workday configuration review to determine a realistic timeframe | BCC Human Resources, Facilities Management Department, MIS, ERP Implementation Team | 3 |
| Create procedures to collect supporting documentation and store it in a centralized location for the interim period until processes are configured within the Workday ERP system. | The Office 365 Form and workflow are in final testing; manual form processing procedures are in place | BCC Human Resources, MIS, Facilities Management | 3,4 |
| Consolidate all procedures into a single manual to provide participating departments with clear SOPs for operations and training. | Interim procedures are in place; the completion of the final document will align with the implementation of Workday procedures | Human Resources, Facilities Management, ERP Implementation Team, MIS | 4 |
| Consult the access control system vendor to ascertain options for configuring holiday schedules. Reconfigure the access control system to support different holiday schedules. | Completed | Facilities Management | 5 |

*Note regarding Finding #3: Although the report cites 70 badges lacking appropriate documentation for changes, 40 of them are not under the Facilities Management Department's oversight. While we are working to implement additional controls, please note that the County may not have jurisdiction over some service areas, including the access control management for some Constitutional Officers.*

**Management & Budget**
500 San Sebastian View, St. Augustine, FL 32084
904.209.0530 | sjcfl.us

**III. Access to the County buildings' secured areas by contractors.**

- ✓ Finding #6: Badges and keys created for continuous contractors are not tracked, and documentation of contractor badge verification is not retained.

The County has various security measures in place for contractors who enter County property to provide services. Services under contract are evaluated during the procurement process, and access control requirements become part of the solicitation scope (background checks, record keeping, etc.). For one-time access, each location can either escort and supervise the contractor on the premises or provide the contractor with a badge for access. After review of all current practices, the one-time contractors are now escorted and supervised on the premises by the designated County staff.

| Actionable Item | Target Time | Responsible staff |
|---|---|---|
| Evaluate procedures for contractors' access to secure areas. | Completed | Facilities Management |
| Deactivate badges for one-time contractors and establish a supervision protocol for contractors entering County-owned buildings to provide approved services. | Completed | Facilities Management |
| Review and update procedures for granting contractors access to County buildings, including secure areas. Update Administrative Code Policy #112 if needed. | In progress | Facilities Management, Building Operations Division, Purchasing |

## IV. Work Orders for control access issues

- ✓ Finding #8: Work orders were not completed in a timely manner.

Staff reviewed the current work order system's functionality and identified procedures to ensure that work order priority levels are assigned accurately and that the work orders are closed in the system immediately after completion to prevent the appearance of unfinished work after the assigned due date.

| Actionable Item | Target Time | Responsible staff |
|---|---|---|
| Evaluate the reporting capabilities of the current work order system. | Completed | Facilities Management |
| Implement procedures to ensure the timely closure of work orders in the system. | Completed | Facilities Management |

As always, St. Johns County remains dedicated to ongoing operational improvements and to ensuring the safety and security of our facilities, employees, and the public.

Please do not hesitate to contact me if you need any additional clarification.

Sincerely,

Olga Rabel,
St. Johns County Compliance Officer