Agenda Item #: 3FF-1

PALM BEACH COUNTY

BOARD of COUNTY COMMISSIONERS

AGENDA ITEM SUMMARY

Meeting Date: **June 9, 2026**

[X] Consent [ ] Regular
[ ] Public Hearing

Department:
Submitted By: County Internal Auditor's Office

I. EXECUTIVE BRIEF

Motion and Title: Staff recommends motion to receive and file:

The Final Audit Report Issued April 22, 2026 as follows:

1. Report #2026-02 Personally Identifiable Information (PII) Data Security

Summary: The County Code requires the County Internal Auditor to submit copies of final audit reports to the Board of County Commissioners (BCC) and the Internal Audit Committee. The final report will be reviewed at the June 17, 2026, Internal Audit Committee meeting. We are submitting this report to the BCC in accordance with the requirements of the County Code. **Countywide (DB)**

Background and Justification: County Code Section 2-463(e)(3) requires the County Internal Auditor to submit copies of final audit reports to both the BCC and the Internal Audit Committee. In addition, County Code Section 2-463(f) requires the submission of these reports. While individual Audit Committee members have reviewed the report, the Internal Audit Committee will formally review it at its next meeting on June 17, 2026. This report is therefore being submitted to the BCC as required by the County Code.

Attachments:

Report #2026-02 Personally Identifiable Information (PII) Data Security

---

Recommended by: _____ 5-1-2026
County Internal Auditor — Date

Recommended by: N/A
County Administrator — Date

II. FISCAL IMPACT ANALYSIS

A. Five Year Summary of Fiscal Impact:

Fiscal Years	2026	2027	2028	2029	2030
Capital Expenditures					
Operating Costs					
External Revenues					
Program Income (County)					
In-Kind Match (County)					
NET FISCAL IMPACT	None	None			
# ADDITIONAL FTE					
POSITIONS (Cumulative)					

Is Item Included In Current Budget? Yes _____ No __X__
Does this item include the use of state funds? Yes _____ No __X__
Does this item include the use of federal funds? Yes _____ No __X__
Budget Account No.: Fund _____ Agency _____ Org. _____ Object _____
Program Number _____ **Revenue Source** _____

B. Recommended Sources of Funds/Summary of Fiscal Impact:

No fiscal impact

A. Department Fiscal Review:

_____

III. REVIEW COMMENTS:

A. OFMB Fiscal and/or Contract Administration Comments:

Budget/OFMB AAP 5/4

Contract Administration 5/5/26 5.5.26

B. Legal Sufficiency:

5/6/26
Assistant County Attorney

C. Other Department Review:

_____
Department Director

This summary is not to be used as a basis for payment.

Office of the County Internal Auditor
Audit Report
Report #2026-02

COUNTYWIDE
PERSONALLY IDENTIFIABLE INFORMATION (PII)
DATA SECURITY

TABLE OF CONTENTS

COUNTYWIDE PERSONALLY IDENTIFIABLE INFORMATION (PII) DATA SECURITY REPORT # 2026-02

AUDIT OBJECTIVE AND CONCLUSION

Objective

We performed this audit to determine:

Did Palm Beach County Administration establish countywide (1) policies and procedures, and (2) training and awareness for staff regarding the protection of Personally Identifiable Information (PII) to ensure that PII collected and maintained countywide is adequately secured in accordance with the National Institute of Standards and Technology (NIST) SP 800-122 as of August 31, 2025?

Conclusion

At the time of the audit, the County did not have a comprehensive countywide framework for protecting personally identifiable information (PII). Specifically, a countywide policy had not been established, responsibility for overseeing PII protection had not been formally assigned, and standardized training had not been implemented.

During the audit, County Administration issued a countywide PII data protection policy, designated a County PII Security Officer to administer the policy, and began development of standardized countywide PII training. These actions significantly improve the County's control environment related to the protection of sensitive information by establishing guidance, accountability, and oversight at a countywide level.

Standardized training has not yet been implemented; therefore, additional work is needed to ensure staff with access to PII understand and follow County requirements for protecting sensitive information. Once training is implemented and departments incorporate the new policy into their procedures, the County will have a more complete framework for protecting personally identifiable information.

AUDIT FINDINGS AND RECOMMENDATIONS

Finding #1 There is no comprehensive countywide PII data security policy that addresses the collection (data minimization), maintenance, and destruction of PII in both physical and electronic formats.

Condition
County Administration advised that the County does not currently have a countywide PPM specifically addressing the protection of PII. We reviewed applicable Countywide PPMs, as well as PPMs from the 15 departments identified as highest risk based on the type and volume of PII collected. Based on this review, we did not identify any PPMs that established a comprehensive set of minimum requirements governing the collection (including data minimization), use, storage, sharing, and disposal of PII in both hard copy and electronic formats.

Effect or Risk
Without standardized training, staff may not fully understand what constitutes Personally Identifiable Information (PII) or how to consistently apply safeguards, increasing the risk that PII is not uniformly protected throughout the County.

Cause
County Administration has not formally designated a specific individual or department responsible for creating and administering a countywide PII policy.

Criteria
National Institute of Standards and Technology (NIST) SP 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information*, Section 4.1.1, requires organizations to develop comprehensive policies and procedures governing the handling of PII at the organization, program, and system levels, as applicable.

Recommendations:

1. The County Administrator should ensure a comprehensive countywide PII data protection policy is developed that establishes minimum requirements for the collection (data minimization), use, storage, sharing, and disposal of both hard copy and electronic PII.

2. The County Administrator should designate the department/individual responsible for administering the newly created PII policy.

Management Comments and Our Evaluation

Management agrees with the finding and recommendations. In responding to a draft of this report, management stated that a countywide Personally Identifiable Information (PII) data protection policy has been issued as PPM

CW-P-088 and that a County PII Security Officer has been designated to administer the policy.

Internal Audit confirmed that PPM CW-P-088 was issued and that responsibility for administering the policy was formally assigned. These corrective actions address the recommendations. The policy was issued and responsibility was assigned after the audit period; therefore, Recommendations 1 and 2 are considered implemented.

Finding #2 The County has not established a countywide standardized PII data security training requirement.

Condition
Based on interviews with County Administration and management from Human Resources (HR) and Information Systems Services (ISS), we determined that the County does not currently provide standardized, countywide training for staff with access to PII.

Effect or Risk
Without standardized training, staff may not fully understand or consistently apply PII safeguards, increasing the risk that PII is not uniformly protected throughout the County.

Cause
County Administration has not formally assigned responsibility for developing and administering countywide PII training.

Criteria
National Institute of Standards and Technology (NIST) *Special Publication (SP) 800-122 Guide to Protecting the Confidentiality of Personally Identifiable Information PII" Executive Summary section*, states "Organizations should reduce the possibility that PII will be accessed, used, or disclosed inappropriately by requiring that all individuals receive appropriate training before being granted access to systems containing PII."

Section 4.1.2 Awareness, Training, and Education states, "An organization should have a training plan and implementation approach, and an organization's leadership should communicate the seriousness of protecting PII to its staff. Organizational policy should define roles and responsibilities for training; training prerequisites for receiving access to PII; and training periodicity and refresher training requirements. To reduce the possibility that PII will be accessed, used, or disclosed inappropriately, all individuals that

have been granted access to PII should receive appropriate training and, where applicable, specific role-based training."

Recommendations:

3. The County Administrator should ensure that standardized countywide PII data security training is established.

4. The County Administrator should designate the department/individual responsible for administering countywide training and awareness for staff related to the newly created PII policies and PII protection requirements.

Management Comments and Our Evaluation

Management agrees with the finding and recommendations. In responding to a draft of this report, management stated that standardized countywide PII data security training is currently being developed and is expected to be implemented later this year, and that responsibility for administering training has been assigned.

Internal Audit confirmed that responsibility for administering countywide PII training has been assigned. This corrective action addresses Recommendation 4; however, the standardized training program has not yet been implemented.

Recommendation 3 will remain open pending development and implementation of the countywide training program. Follow-up will be necessary to confirm that training has been developed, implemented, and is being delivered to staff with access to PII.

OPERATIONAL STRENGTHS

The County Administrator and Chief Deputy County Administrator expressed receptiveness to audit feedback and a commitment to continuous improvement. As a result of discussions held during the audit, they indicated that development of a new countywide PII data security policy (PPM) is currently underway. However, the policy was not finalized or implemented as of the audit period.

BACKGROUND

Personally Identifiable Information (PII) includes information that can be used to identify an individual, such as names, Social Security numbers, driver's

license numbers, dates of birth, financial account information, medical information, and other sensitive personal data. Many County departments collect, maintain, and store PII as part of their operations.

Improper collection, storage, transmission, or disposal of PII increases the risk of unauthorized disclosure, identity theft, fraud, reputational damage, and potential legal liability for the County. Protecting PII requires consistent policies, procedures, training, and oversight across departments.

During prior audit work and reviews conducted across various County departments, Internal Audit observed that departments collect and maintain PII in various formats and systems, and that practices related to the collection, storage, and protection of PII were not applied consistently across departments. These observations indicated a potential countywide risk related to the protection of sensitive information.

At the time of this audit, the County did not have a comprehensive countywide policy or standardized training related to the protection of PII. Responsibility for overseeing PII protection at a countywide level had not been formally assigned, and departments were responsible for developing their own practices.

During the audit, County Administration developed and issued a countywide Personally Identifiable Information (PII) data protection policy and designated a County PII Security Officer to administer the policy. Administration also began development of standardized countywide PII training. These actions establish a countywide governance framework for protecting sensitive information, including policy guidance, oversight responsibility, and training expectations. The effectiveness of this framework will depend on implementation and compliance across departments, which may be evaluated during future audit work.

AUDIT SCOPE AND METHODOLOGY – GENERAL

Scope

The audit scope covered countywide and departmental policies and procedures in place as of August 31, 2025

Methodology

Based on the County's 2025 organizational chart, the County has 29 departments. We obtained PII-related risk assessment surveys from all 29

departments. Using survey responses, we requested additional information regarding the types and volume of PII collected and classified the data into three risk-based categories: (1) Sensitive (Green), (2) Private (Yellow), and (3) Restricted (Red), which includes data such as dates of birth and Social Security numbers.

Departments were assigned high, medium, or low risk ratings based on both the volume and sensitivity of PII collected. Using this methodology, 16 of the 29 departments were ranked as high risk. One of the 16 departments, the Office of Equal Business Opportunity (OEBO), no longer exists; therefore, we reviewed the policies of the remaining 15 high-risk departments.

Note: OEBO is now a division within Housing and Economic Development (HED). HED policies were reviewed as part of this methodology.

Risk Ranking Summary

- High Risk: 15 departments
- Medium Risk: 9 departments
- Low Risk: 2 departments
- No PII: 2 departments

Because the County does not have a comprehensive countywide PII policy, we focused the engagement on identifying gaps in existing policies related to the collection, use, storage, and disposal of PII, rather than reviewing individual transactions or processes.

Our methodology included:

- Interviewing County Administration and management from the 15 departments ranked as high risk to obtain and review department-level and countywide policies and procedures. This review assessed whether existing policies adequately address staff responsibilities related to PII protection, confidentiality, retention, and the reporting of PII breaches in accordance with NIST standards.
- Interviewing Human Resources (HR) management to determine whether new employees are required to review PII disclosure or confidentiality documents as part of the onboarding process and whether County staff receive training related to the proper collection, use, storage, or destruction of PII.
- Interviewing Information Systems Services (ISS) management to determine whether County staff receive training related to their responsibilities for PII protection.

- For benchmarking purposes, contacting eight similar sized Florida counties to determine whether they have a countywide PII data protection policy or a centralized data governance function. (This was done for planning/context only. NIST remains the basis for our audit findings.)

AUDIT METHODOLOGY – DETAIL BY AUDIT FINDING

Finding #1 Internal Audit reviewed applicable countywide Policy and Procedure Manuals (PPMs) and PPMs from the 15 departments identified as highest risk based on the type and volume of PII collected to determine whether any established a comprehensive set of minimum requirements governing the collection (including data minimization), use, storage, sharing, and disposal of PII in both hard copy and electronic formats, consistent with NIST SP 800-122.

Internal Audit also obtained and reviewed department-level PII policies and considered information obtained during prior audits indicating that PII protection practices were not applied consistently across all County departments.

Finding #2 Internal Audit reviewed onboarding procedures and training practices with Human Resources (HR) and Information Systems Services (ISS) to determine whether standardized countywide training related to PII protection was required or provided to staff with access to PII.

MANAGEMENT AND AUDIT RESPONSIBILITIES

Management is responsible for establishing and maintaining effective internal controls to help ensure that appropriate goals and objectives are met; resources are used effectively, efficiently, and economically, and are safeguarded; laws and regulations are followed; and management and financial information is reliable and properly reported and retained.

Internal Audit is responsible for using professional judgment in establishing the scope and methodology of our work, determining the tests and procedures to perform, conducting the work, and reporting the results.

We conducted this performance audit in accordance with generally accepted government auditing standards. These standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit

objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

David Zamora, CIA, CRMA, CFE, CGAP, CFI
County Internal Auditor
April 22, 2026

Palm Beach County
Board of County Commissioners
P.O. Box 1989
West Palm Beach, FL 33402-1989
(561) 355-2201
www.pbc.gov

April 1, 2026

Mr. David Zamora
County Internal Auditor
2300 N Jog Road
West Palm Beach, FL 33411

Dear Mr. Zamora,

Thank you for the opportunity to review and respond to Audit Report #2026-02 regarding Countywide Personally Identifiable Information (PII) Data Security.

Palm Beach County Administration appreciates the work performed by the Internal Audit Office and acknowledges the importance of establishing strong, consistent controls over the protection of PII across all departments.

In response to the audit findings:

Finding #1 – Countywide PII Policy
The County has addressed this finding. A comprehensive countywide Policy and Procedure Manual (PPM) governing the protection of Personally Identifiable Information (PII) was formally developed and implemented on February 25, 2026. The new PPM is CW-P-088 (See Attachment). This policy establishes minimum requirements for the collection (including data minimization), use, storage, sharing, and disposal of PII in both physical and electronic formats. Responsibility for administration of this policy has also been designated in the PPM to Michael Butler, Deputy Chief Information Officer.

Finding #2 – Countywide PII Training
As part of the new PPM, the County Administrator has established a training component for Department Heads, Supervisors, and employees.

The County is actively working to establish this standardized training. The County is currently collaborating with Proofpoint, our email security vendor who currently provides our security training. Proofpoint also provides PII protection and training that will be part of the new standardized security training established for county employees.

The new standardized countywide training program will focus on PII data security and awareness and will be included as a component of the overall security training.

It will include the following components:

- What qualifies as PII and examples in everyday work contexts.
- How to store, transmit, and share PII securely (access, email, cloud, paper).
- Avoiding common PII exposure risks (phishing, misdirected email, unsafe storage, social engineering).
- Employee responsibilities under privacy laws and internal data protection policies, often reinforced with short quizzes and interactive scenarios

It is expected to be finalized and made available for use by County departments later this year.

Palm Beach County Administration remains committed to strengthening its data governance framework and ensuring alignment with applicable standards, including NIST SP 800-122. We appreciate the audit team's recommendations and will continue to implement improvements to enhance the protection of sensitive information across the organization.

If you have any questions or require additional information, please do not hesitate to contact our office.

Sincerely,

Todd J. Bonlarron
Chief Deputy Administrator
Palm Beach County

Cc: Joseph Abrozzo, County Administrator
Michael Butler, Deputy Chief Information Officer