Fairfax County Internal Audit Office

Retirement Administration Agency (RAA)
Data Protection Audit
Final Report
May 2022

"promoting efficient & effective local government"

Background

Agencies within the Fairfax County Government are responsible for handling sensitive and confidential information during the normal course of operations. Departments and agencies are required to determine the nature and extent of security and system controls that must be implemented to protect data in information systems in compliance to the County Department of Information Technology (DIT) *Information Technology (IT) Security Policy 70-05.01v8.* The Internal Audit Office (IAO) has developed a standardized audit plan to review internal controls over data classification and security of confidential or sensitive information used and stored by individual departments/agencies.

Executive Summary

Our audit focused on controls over classifying department's data based on the level of sensitivity and their controls to protect confidential records. Additionally, we reviewed access to information to ensure it was based on a business need with least privileges access rights. Our audit population included the three systems Retirement Administration Agency (RAA) operates.

RAA uses the County owned Pension Gold System (PG) to maintain active members payroll information; calculate and setup member's retirement benefits; and, process retirees' pension and inactive members' refunds. RAA uses the Laserfiche Scan System to scan and store files to the system as images. The Laserfiche Scan System is integrated with PG, allowing the user to view scanned images while using PG. Lastly, RAA uses the Fairfax County Pension Gold System Web Member Service System that allows members to view retirement and beneficiary information, estimate member's retirement benefit, and to view a retiree's pension.

In general, RAA staff was knowledgeable of *IT Security Policy 70-05.01v8* requirements to protect data processed on the County owned systems. Users access rights to systems were granted based on their job responsibilities. Physical pension-related documentation was secured in a locked room with restricted access. RAA informally implemented proper controls over access and changes to confidential and sensitive data. However, we did note some areas where RAA could strengthen their internal control effectiveness:

- Develop written department specific information security policies and procedures for its applications that contain confidential/sensitive information.
- Develop and implement a User Access Authorization form or SharePoint workflow program to formally document the creation, modification, and approval of user accounts for the Pension Gold and Laserfiche systems.
- Perform periodic review of the users lists for the PG and Laserfiche systems and ensure user access is aligned with employees' job responsibilities.
- Ensure RAA's Zoom account security settings comply with DIT guidance while the application is still in use.

Scope and Objectives

This audit was performed as part of our fiscal year 2022 Annual Audit Plan and was conducted in accordance with generally accepted government auditing standards. Those 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. The objectives of the audit were to determine the adequacy of controls over:

- Development of Retirement Administration Agency data protection processes,
- Compliance to County Information Security policy and external regulations for data identification, classification, and protection for all systems,
- Access and changes to confidential and sensitive data,
- Disclosure of data.

Methodology

Our audit approach included review of *Information Technology Security Policy 70-05.01v8*, the *U.S. Department of Commerce - National Institute of Standards and Technology (NIST) Special Publication (SP) 800-122 Guide to Protecting the Confidentiality of Personally Identifiable Information, Policy and Procedures for Portable Storage Devices (USB Flash Drives)* and other online meeting tool policy and procedures to gain an understanding of data classification determination methodology and best practices for protecting confidential data. We interviewed department staff responsible for data classification policies and procedures, system user access, practices for the disclosure, and protection of sensitive or confidential data. We obtained a list of the systems the RAA operates and determined the reasonableness of data classification. In addition, we conducted system walk-throughs, reviewed user requests for access and removal of access for terminated/transferred employees, determined if access was appropriate for users, and reviewed system audit trail logs.

The Fairfax County Internal Audit Office (IAO) is free from organizational impairments to independence in our reporting as defined by Government Auditing Standards. We report directly and are accountable to the County Executive. Organizationally, we are outside the staff or line management function of the units that we audit. We report the results of our audits to the County Executive and the Board of Supervisors, and IAO audit reports are available to the public.

Findings, Recommendations, and Management Response

1. Internal Written Policies and Procedures

Retirement Administration Agency (RAA) did not have written information security policies and procedures for its agency-specific applications that contain confidential/sensitive information.

Per DIT's Information Security Office (ISO), the Agency's Information Security Coordinator (AISC) is responsible for coordinating the development and maintenance of agency-specific information security policies, standards, and procedures.

In addition*, NIST SP 800-53, Security and Privacy Controls for Information Systems and Organizations, Section 3.13, Program Management states: "Organizations document program management controls in the information security and privacy program plans. The organization-wide information security program plan and privacy program plan supplement system security and privacy plan developed for organizational information systems."*

Lack of agency-specific information security policies and procedures for agency applications with sensitive and confidential information increases the risks of agency systems not having proper access controls and unauthorized disclosure of system's confidential or sensitive information that may result in security breaches and unauthorized access.

Recommendation: RAA should develop internal written information security policies and procedures for its agency-specific applications. The policies and procedures should include processes for authorizing, granting, approving, and terminating system user access. Additionally, the disclosure, use, storage, and destruction of sensitive/confidential information should be addressed. The policies and procedures should be reviewed and approved by DIT ISO.

Management Response: RAA will develop internal written information security policies and procedures for the agency specific systems. The policies and procedures will also include information about the newly established User's Access Authorization Form as a tool to grant approval or, to terminate a user's access to the agency specific systems. Key areas which will be addressed are system use, storage and destruction of confidential information. DIT ISO will be involved in the finalization for this recommendation, therefore, the deadline for this response is in two parts. Part 1 – Completion of the policies and procedures by RAA. The draft policies and procedures will be submitted to DIT ISO for review. Part 2 – Submission, review, and approval by DIT ISO. Management anticipates completing Part 1 actions by June 3, 2022.

2. User's Access Authorization Form

RAA did not utilize a user's access authorization form to ensure proper documentation of business justifications and approval for system access. They did have an informal process that utilized emails to document the requests and approvals for account creation. However, the Pension Gold and Laserfiche system administrator did not retain all emails to document the approval of new system accounts. Additionally, their informal process was not documented.

Information Technology Security Policy 70-05 01, Section 3.5.1 Access Control states: "Authorization to create a user ID and password must be received from a designated approval authority…… Requests for user, administrative, and system access must be approved according to formal access request procedures."

Additionally, *NIST Special Publications SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information, Section 4.3 Security Controls* states: "Organizations can control access to Personally Identifiable Information (PII) through access control policies and access enforcement mechanisms (e.g., access control lists)." A form of access control is to document the appropriateness of the access granted to individuals, this is best done through the completion and approval of an access request form. This will evidence the need for access and the approval of the access.

If a user access form is not used, system access may be granted without the necessary information to ensure users' access granted to confidential/sensitive information is appropriate. There is a risk that access could be improperly granted to an unauthorized individual who does not require this information to complete their daily duties putting confidential data at risk for misuse. Misuse of data could be the theft, alteration or destruction of confidential data or inappropriate access.

Recommendation: We recommend that RAA develop and implement a User Access Authorization form or SharePoint workflow program to formally document the creation, modification, and approval of user accounts for the Pension Gold and Laserfiche systems. The form or workflow data should be maintained on file in the agency.

Management Response: RAA will finalize the draft version of the Retirement Systems' User's Access Authorization Form. RAA Managers will be introduced to the Authorization form during the RAA Managers meeting. Discussion will include the importance and proper use of the Authorization form. Additionally, "How To Use" the Authorization form will be discussed. Management anticipates completing these actions by May 31, 2022.

3. Periodic Review of System Users

The Retirement Administration Agency did not have formal procedures requiring the periodic review of system users to determine if user access was legitimate. We found one Pension Gold *s*ystem user, out of 25 active user accounts tested, for which access was not needed and another user who was not in the correct group within Pension Gold. Additionally, there was no formal process in place to notify the system administrator of changes to user access.

The Information Technology Security Policy 70-05 01 Section 3.5.2 Account Administration states: "User access to Fairfax County systems shall be periodically reviewed and adjusted as necessary by the system owners to ensure that access is in accordance with the concept of least privilege. Agency Information Security Coordinators, Access Control Administrators, or other designated personnel shall review and adjust access privileges when the role or responsibilities of a user changes or the user no longer needs access to County information systems or applications."

Unauthorized users' access to a system increases the risk of unauthorized disclosure and use of critical or sensitive information.

Recommendation: We recommend that RAA establish procedures requiring the appropriate staff to periodically review all of their system users lists and notify the system administrator when an employee is terminated, transferred or no longer authorized to use the systems. The access for all improper users should be removed. The review should be documented, and initialed/dated by the reviewer.

Management Response: RAA will establish a procedure that require RAA Managers to periodically review user lists of RAA user accounts associated with the agency specific systems. This periodic review will ensure that the user accounts are both current and accurate. If there are modifications to the list, the Manager would use the User's Access Authorization Form referenced in Recommendation #2 to identify user accounts that require remediation. Management anticipates completing these actions by May 20, 2022.

Note: During the audit, IAO verified that RAA revised the two employees' access, therefore, no follow-up will be performed for this item. However, follow-up will be performed on the procedures.

4. Zoom Account Settings

The RAA's Zoom host account security settings reviewed did not comply with the DIT Zoom accounts requirements. RAA used Zoom for public Retirement Services Board meetings. We compared the Fairfax County Zoom Requirements set forth by DIT in April 2020 to the RAA Zoom account meeting settings and noted eight meeting settings that did not comply:

a. "Embed Password in meeting links" was not disabled.
b. E2E Encryption for all sessions, including 3rd party endpoints was not required.
c. Participants were allowed to save chats.
d. File sharing options via meeting chat was not disabled.
e. Feedback to Zoom was not disabled.
f. Co-host feature was not disabled.
g. Participant local recording was not disabled.
h. Cloud recording was not disabled.

Agencies using Zoom host accounts must comply with the Fairfax County Zoom Requirements. Also*, NIST SP 800-128, Guidelines for Security-Focused Configuration of Information Systems, Section 2.1.3, Role of Security-Focused Configuration Management states: "The configuration of a system and its components has a direct impact on the security posture of the system. How the configurations are established and maintained requires a disciplined approach for providing adequate security."*

Additionally, the *Fairfax County Zoom Requirements states "Fairfax County requires the meeting host to follow and implement these settings on each meeting."*

Noncompliance with the County Zoom requirements increases the risks of eavesdropping on Zoom meeting conversations; meeting chats/documents that are not properly encrypted; and the sharing of files that my contain malware. This could result in unauthorized access to confidential or sensitive information exchanged or discussed in Zoom meetings.

Recommendation: RAA should configure the security settings to comply with the Fairfax County Zoom Requirements or document the reason why the settings cannot be applied. Additionally, RAA should periodically review Microsoft Teams functionality to determine if it will meet their operational requirements to replace the use of Zoom as DIT prefers County staff use of MS Teams for video conferencing for better application support and security.

Management Response: The Executive Director of RAA is the administrator of the Zoom account. He updated the settings and thus completed this requirement.

Note: *During the audit, IAO verified that RAA updated their Zoom account security settings, therefore, no follow-up will be performed for this item.*