Fairfax County Internal Audit Office

Fairfax County Public Library
Data Protection Audit
Final Report
October 2022

NOTE: ***Selected sensitive and confidential operational and security information will be omitted from public disclosure, based on the Virginia Freedom of Information Act (FOIA) Va. Code Ann. 2.2-3705.2(14)(b). This information, if disclosed, would subject the County to potential computer data security risks.***

"promoting efficient & effective local government"

Background

Data protection is a set of strategies and processes to ensure the privacy, availability, and integrity of data, and to secure data from corruption, compromise, or loss. Protecting data on county information systems is a dual responsibility between the Department of Information Technology (DIT) and agencies/departments. DIT is the primary custodian of data and information for agencies/departments and agencies/departments are the owners of their data.

Per the County Department of Information Technology (DIT) Information Technology (IT) Security Policy 70-05.01v8, as data owners, agencies/departments are responsible for defining and implementing processes for information security controls such as properly classifying data, establishing agency-specific procedures for system access control, reviewing security logs, and resetting passwords in their departments. Agencies/departments should ensure the security and privacy of their data, regardless of medium; and, that it is used, maintained, disclosed, and disposed of according to laws, regulations, policies, and standards.

The Internal Audit Office (IAO) has developed a standardized audit plan to review and assess departments/agencies' internal controls over data protection and security of confidential and/or sensitive information used and stored.

Executive Summary

Our audit focused on controls over data protection for the Fairfax County Public Library's (FCPL) data for sensitive/confidential records. Additionally, we reviewed access to information to ensure it was based on a business need with least privileges access rights. Our review included the two systems with sensitive information that FCPL operates: Polaris and Databank.

FCPL uses the Polaris system, an integrated library management system, to process library applicant information; to checkout public library material; and, to provide customer service by FCPL personnel. FCPL uses Databank, a cloud-based system, to store human resource and financial PDF file records.

In general, FCPL staff was knowledgeable of *IT Security Policy 70-05.01v8* requirements to protect data processed on the County systems. Users access rights to systems were granted based on their job responsibilities. However, we did note some actions FCPL could take to strengthen their internal controls over data protection:

- Document their information security procedures in formalized written policies and procedures for their agency specific applications (Polaris and Databank) that contain confidential/sensitive information.
- Perform a periodic review of the user lists for the Polaris and Databank systems to ensure user access is still appropriate.

- 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 Databank system.
- Perform periodic reviews of permissions to X: and S: share drives. There were three individuals with permissions to folders on FCPL share drives that did not need access. One individual transferred to another County agency, and the other two individuals no longer worked for the County. Some of these folders contained confidential/sensitive information.
- [redacted]

[redacted]

- Document in a memo how FCPL specific data stored in the Databank and Polaris system is classified. The memo at a minimum should indicate that the department uses data classification criteria from *IT Security Policy 70-05.01v8* to classify its data.

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 Fairfax County Public Library 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 FCPL operates and determined the reasonableness of data classification. In addition, we conducted system walk-throughs; reviewed user requests for access; removal of access for terminated/transferred employees; and determined if access was appropriate for users.

The Fairfax County Internal Audit Office 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

The Fairfax County Public Library (FCPL) did not have written information security policies and procedures for its agency-specific applications that contain confidential/sensitive information: Polaris and Databank systems.

The Information Technology Security Policy 70-05 01 states: “ Agency management responsibilities shall include ….Developing an agency-specific IT Security Policy anchored to the agency’s business needs and in compliance with the County’s IT Security Policy and enterprise-wide IT and other policies.”

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 which may result in unauthorized disclosure of system’s confidential or sensitive information, security breaches, and unauthorized access.

Recommendation: FCPL should develop internal written information security policies and procedures for its agency-specific applications (Polaris and Databank) that contain confidential and sensitive information. 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: FCPL will have meetings with appropriate agency staff to discuss the disclosure, use, storage, and destruction of sensitive and confidential information for the Polaris and Databank systems. FCPL will develop internal written security policies and procedures for Polaris and Databank, including processes for authorizing, granting, approving, and terminating system user access. The policies and procedures will be sent to DIT for approval. Management anticipates completing these actions by June,1 2023.

2. Periodic Review of System Users

The Fairfax County Public Library did not have formal procedures requiring the periodic review of system users to determine if user access was appropriate. We found 4 users with access to Databank system that currently work for other County agencies and 12 users with access to Polaris system who no longer work for the County. 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."

Lack of periodic reviews of user access privileges increase the risk of unauthorized users' access to a system which may lead to unauthorized disclosure and use of critical or sensitive information.

Recommendation: We recommend that FCPL establish procedures requiring the appropriate staff to periodically review their system user's 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: FCPL will establish formal, written procedures for review of system user lists every six months for the Polaris, and Databank systems to be completed for the months of January and July. Management anticipates completing these actions by February 1, 2023.

3. User's Access Authorization Form

FCPL did not have proper access authorization documentation for 10 of the 11 eleven users tested. FCPL did not utilize a user's access authorization form to ensure proper documentation of business justifications and approval for access to the Databank system. While FCPL did have an informal process that utilized emails to document the requests and approvals for account creation, these emails were not being retained 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."

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. This increases the risk of unauthorized access putting confidential data at risk for theft, alteration/destruction, or inappropriate access.

Recommendation: We recommend that FCPL develop and implement a User Access Authorization form or workflow application to formally document the creation, modification, and approval of user accounts for the Databank system. The form or workflow application data should be maintained on file in the agency.

Management Response: FCPL will expand the current Polaris user ID request form to include Databank requests. Management anticipates completing these actions by December 1, 2022.

4. Shared Folders

There were two individuals with permissions to a FCPL Financial Services Division shared folder and one individual with permissions to a FCPL X: drive shared folder that no longer needed access. One employee transferred to another County agency. The other two individuals no longer worked for the County. Also, there were two files on the FCPL's S: drive that contained Personally Identifiable Information (PII). One file was last accessed in 2011 and contained library card applicants name, address and date of birth, and another file last accessed in 2009 contained employee name, date of birth, and salary information. Per FCPL IT management, all branch staff had access to those files.

While the access to these folders was appropriate when they were created, at the time of the review these individuals no longer needed to access the information in the folders. Additionally, FCPL did not have written procedures that outlined the creation, access approval/removal or monitoring of the S: or X: shared drive folders.

DIT Security Policy 70-05 01, Section 3.5.1 states: "Data and system owners shall implement operational procedures and technical controls to ensure access to Fairfax County Government information and systems is based upon the principle of least privilege and an authorized need to know and access."

If confidential information is accessed by an unauthorized individual, the risk that the information could be compromised increases, either intentionally or accidentally.

Recommendation: FCPL should periodically review their X: and S: shared drives' access permissions for appropriateness. We recommend FCPL immediately remove the PII information stored in their shared folders determined to be no longer needed. In addition, FCPL should consider using automated tools to analyze the S: and X: drives for PII files which access may be no longer needed. Finally, FCPL should develop written internal policies and procedures for granting/removing access to their shared folders and how confidential data should be stored on them.

Management Response: With the assistance of DIT, FCPL will review all documents and permissions for FCPL's S: drives and X: drives. As needed, documents will be deleted, and permissions will be edited. FCPL will develop written, internal policies for granting and removing access to shared folders. This policy will include procedures for storing confidential data on shared folders, and a schedule for annual review of these shared folders. Management anticipates completing these actions by December 12, 2023.

5. [redacted]

[redacted]

[redacted].

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

6. [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]