Richmond City Council

The Voice of the People — Richmond, Virginia

Office of the Inspector General

September 15, 2021

Mr. Lincoln Saunders
Acting Chief Administrative Officer
City of Richmond

The Office of the Inspector General (OIG) has completed an investigation within the Department of Social Services. This report presents the results of the investigation.

Allegations

The Office of the Inspector General initiated an Investigation involving two Department of Social Services (DSS) employees who used the login and password of an employee without their knowledge or permission.

Legal and City Policy Requirements

1) In accordance with the Code of Virginia §15.2-2511.2, the Inspector General is required to investigate all allegations of fraud, waste and abuse.
2) City Code section 2-231 requires the Office of the Inspector General to conduct investigations of alleged wrongdoing.
3) Administrative Regulations 2.5 Electronic Media Systems (internet and intranet) Security Section III Procedure – (G) "Never use another individual's account."

Findings

The investigator identified the two employees. Employee one is a Deputy Director and employee two is a Business System Analyst both assigned to the Department of Social Services.

The investigator interviewed the complainant who stated upon arriving at a training session in the DSS training room he/she observed that someone had logged into Harmony using their user name and password and it was displayed on the screen in the training room. The complainant also stated that the Business System Analyst also logged in as another employee who was not attending the training.

The investigator interviewed the Deputy Director who admitted an employee login and password was changed and used in the training environment of Harmony. This was done because the employee had material in their training module that was used for training. Some employees who attended the training were new and had no material in

their training module. The Deputy Director further stated this was permissible to do as long as it was done in training mode this was in their policy. The Deputy Director also confirmed that a second employee who did not attend the training login and password was changed and used during the training. Neither of these employees was asked if their login and password information could be used prior to the training session. This is a violation of Administrative Regulations 2.5 Electronic Media Systems (internet and intranet) Security Section III Procedure – (G) "Never use another individual's account."

The investigator interviewed the Business Systems Analyst who admitted to using an employee login and changed the password for the training session. This was done in the training mode of the Harmony. The analyst said this was done to show data to the new employees that were attending the training who did not have any data in their training module. The analyst also stated that another employee's login and changed password was used during the training session and neither employee was asked if their login and password could be used. The analyst said neither employee's login nor password was used in the live mode. This is a violation of Administrative Regulations 2.5 Electronic Media Systems (internet and intranet) Security Section III Procedure – (G) "Never use another individual's account."

The analyst stated this was ok to do in the training module and the Deputy Director was present during the training and advised the analyst which employee's information to use for login.

The Department of Information Technology was contacted who confirmed that Administrative Regulation 2.5 mentions "Never use another individual's account". The Regulation does not mention production or non-production. Also, since the non-production data was most likely refreshed from the production database, using another's person credentials even in a non-production instance could give that person access to data they otherwise would not have had had they used their credentials. The best practice for training is to set up training accounts or have the person available during the training and have them conduct or present for that portion of the training.

Conclusion

Based on the findings, the OIG concludes that the allegation is substantiated against the Deputy Director and Business System Analyst for violating Administrative Regulation 2.5 Electronic Media Systems (internet and intranet) Security Section III Procedure – (G) "Never use another individual's account."

Recommendation

The OIG recommends the Department of Social Services take appropriate disciplinary action on the Deputy Director and the Business System Analyst for violation of City of Richmond Administrative Regulations 2.5 Electronic Media Systems (internet and intranet) Security Section III Procedure – (G) "Never use another individual's account."

Should you have any questions, please contact me at extension 1840.

Submitted,

James Osuna
Inspector General

CC: Reginald Gordon, DCAO Human Services
Shaunda Giles, Director of Social Services
Charles Todd, Director of Information Technology
Honorable Members of City Council