REPORT OF EXAMINATION | 2017M-282

Newark Housing Authority

Information Technology

MARCH 2018

OFFICE OF THE NEW YORK STATE COMPTROLLER
Thomas P. DiNapoli, State Comptroller

Contents

Report Highlights

Newark Housing Authority

Audit Objective

Determine whether the Board and Authority officials have established policies and procedures to adequately safeguard information technology (IT) assets.

Key Findings

- The Board did not adopt IT policies and procedures to address acceptable computer use, individual access rights, disaster recovery and password security management.
- Authority officials did not ensure the network accounts for six former personnel had been deactivated.

Key Recommendations

- Adopt policies and procedures to address acceptable computer use, user access rights, disaster recovery and password security management.
- Ensure the access rights for users no longer employed are revoked.
- Address the IT recommendations communicated confidentially.

Background

The Newark Housing Authority (Authority) is located in the Village of Newark in Wayne County. The Authority is governed by a seven member Board of Commissioners, five are appointed by the Village's Mayor and two are elected by the tenants. The Board is responsible for hiring an Executive Director who is responsible for the general management, supervision and direction of the Authority's day-to-day operations.

The Authority provides affordable, quality housing to low-income individuals and families. The Authority uses a variety of electronic data and computer resources to manage its daily operations.

Quick Facts	
Employees	13
2016-17 Budgeted Appropriations	$3.8 million

Audit Period

April 1, 2015 – August 22, 2017

Information Technology

The Authority uses IT to initiate, process, record and report transactions. It also relies on its IT systems for Internet access, email and maintaining financial information. The Authority has an internal network that allows individuals to share and access electronic data and computer resources. The Authority pays an IT consultant to manage the network upon request. The IT consultant assists the Authority with setting up new computers, network access and trouble-shooting network problems. If IT systems are compromised, the results could range from an inconvenience to a catastrophe and could require extensive effort and resources to evaluate and repair.

What IT Security Policies and Procedures Should the Board Adopt to Safeguard Authority Data?

The Board should adopt a computer policy that defines acceptable use. An effective process for safeguarding the Authority's IT system includes an acceptable computer use policy, which holds users accountable for properly using and protecting Authority resources and defines the procedures for computer, Internet and email use. Additionally, the Board should adopt policies and procedures for granting, revoking, modifying and monitoring individual access rights and a process to monitor and review these rights once granted. To ensure the highest level of security over Authority data, the Board should also adopt policies and procedures for security management. All IT policies and procedures should be periodically reviewed and updated to reflect changes in technology and the Authority's computing environment.

The Board Did Not Adopt IT Security Policies and Procedures

The Board did not adopt policies and procedures for acceptable computer use and granting, revoking, modifying and monitoring individual access rights to the networks through Active Directory (AD). In addition, the Board has not adopted a comprehensive disaster recovery plan or policies and procedures for password security management. We reviewed the server and all 11 computers in use during our audit period. We found that employees accessed non-business related websites and stored personal files on the network.

Additionally, we compared a list of all individuals who have access to the network to payroll reports to determine whether users are currently employed and should have access. We found that six individuals who were no longer employed by the Authority still had active user accounts. If the Board had adopted policies and procedures for revoking access rights, the six individuals who have left the Authority would not have access to the system. In addition, there is an increased risk that the Authority could lose important data and suffer a serious interruption in operations and that unauthorized individuals could access computerized data to copy, manipulate or delete sensitive information.

The Board Did Not Disable or Remove Unnecessary User Accounts

The Board has not implemented a process to address the deactivation of user accounts. The Authority's AD has 19 network user accounts, seven (37 percent) of which are inactive. These inactive user accounts have not been used to logon to an Authority computer in at least six months, with the oldest having a logon date of June 9, 2010. Furthermore, these seven user accounts are still enabled meaning they can still be used and because passwords are set to never expire, they could easily be used to actively logon to the network.

We also found potentially unnecessary local user accounts that are still enabled on the server and on all but two of the computers. A total of 17 of the 27 local user accounts have not been used to logon to the respective computer or server in at least six months. Two of these accounts have never been used and six were last used in 2012 or 2013.

Additionally, generic accounts are accounts that are not associated with a unique individual (based on the common name defined on the account). The use of generic accounts can prevent the Authority from tracing suspicious activity to a specific individual, thus presenting difficulties in holding the responsible user accountable for their actions. Our examination identified five generic accounts on the Authority's network.

Unnecessary user accounts should be disabled or removed as soon as they are no longer needed to decrease the risk of unauthorized access and potential entry points for attackers to copy, manipulate or delete personal, private, and sensitive information (PPSI). Of particular risk are user accounts for former employees, as these could potentially be used for malicious activities. Further, unnecessary accounts create additional work to manage access, along with the risk of errors that could result in users being inadvertently granted more access than needed.

Why Should the Board Provide Security Awareness Training?

Computer users need to be aware of security risks and be trained in practices that reduce internal and external threats to IT systems and data. While IT policies provide guidance for computer users, cybersecurity training helps them understand their roles and responsibilities and provides them with the skills to do it. Training programs should be directed at the specific audience (e.g., system users or administrators) and include the information that attendees need to perform their jobs. IT security awareness should reinforce IT policies and can focus on security in general or some narrow aspect of security (e.g., the dangers of opening an unknown email or attachment or how to maintain laptop security while traveling).

The Board Did Not Provide Security Awareness Training

The Board did not provide users with security awareness training to help ensure they understand security measures necessary to protect the network. As a result, the Authority's IT assets are more vulnerable to loss and misuse.

Why Should the Server Be Secured?

Security controls restrict physical access to computer resources and protect these resources from intentional or unintentional harm, loss or impairment. Such controls include guards, gates, and locks and also environmental controls such as smoke detectors, fire alarms and suppression, protection from water damage and uninterruptable power supplies. Authority officials must ensure that the server is located in a secure location and implement procedures to ensure that physical access is controlled.

The Authority Did Not Properly Secure the Server

Authority officials did not ensure that the server was in a secure location. The Authority's server is located on the floor in an employees' office that is unlocked during the day.[1] Leaving the server on the floor makes it more susceptible to water damage and damage from other inadvertent causes. However, the Authority did have the server connected to an uninterruptable power source.

Why Should the Authority Maintain a Software Inventory?

In order to safeguard assets and data, it is essential to manage software and licenses. Therefore, Authority officials must have an understanding of the software they own, how it is used and how best to track user rights to ensure licensing compliance. Software inventory records should include an item's description including its version and serial number, a description of the computer on which the software is installed and any pertinent licensing information. The effective management of software also includes ensuring that only appropriate business software is installed to reduce the risk of unwanted consequences and unnecessary costs that could result from unauthorized software. Additionally, to reduce vulnerabilities, Authority officials must ensure that software and patches are up-to-date.

1 The backdoor to the Authority is locked during the day and the front door is only open during business hours.

The Authority Did Not Maintain an Inventory of Its Software

The Authority did not maintain an inventory of its software. Without a complete and comprehensive software inventory, the Board cannot ensure that all the software programs running on its computers are properly licensed and are for legitimate business purposes. Additionally, our testing of the server and 11 computers found non-business software applications including weather programs, a browser hijacker and extended toolbar as well as a shopping application. These non-business applications not only provide additional opportunities for malicious attacks but also indicate a lack of productivity if employees are using these applications during the workday.

Why Should the Authority Assign Unique Login Credentials to Each Financial Application User?

Effective access controls require that financial system user accounts be linked to specific individuals to help prevent and detect unauthorized or inappropriate activity. Users should not be allowed to share accounts. Further, access within the application should be assigned based on the users' job responsibilities.

The Authority Did Not Assign Unique Login Credentials to Each Financial Application User

Three employees use the Authority's financial application and share one user account. Because two of the three users do not routinely use the application, officials believed that it was acceptable for them to share the common user account. When shared accounts are used, accountability is diminished and activity in the system may not be able to be traced back to a single user.

Why Should the Authority Have a Disaster Recovery Plan?

The Board should adopt a disaster recovery plan to describe how Authority officials will deal with potential disasters that affect the IT system. A disaster recovery plan provides a framework for reconstructing vital operations to ensure that time-sensitive operations and services can be resumed in the event of a disaster. Disasters may include any sudden, unplanned catastrophic event (e.g., fire, computer virus or inadvertent employee action) that compromises the availability or integrity of the IT system and data. Typically, a disaster recovery plan involves an analysis of business processes and continuity needs, a focus on disaster prevention, the roles of key individuals and the precautions to maintain or quickly resume operations. Additionally, the disaster recovery plan should include data backup procedures and periodic testing of the backups to ensure they will function as expected. The plan should be distributed to all responsible parties, periodically tested and updated as needed.

The Authority Does Not Have a Disaster Recovery Plan

The Board did not develop a formal disaster recovery plan to address potential disasters. Consequently, in the event of a disaster, Authority officials have no guidelines to minimize or prevent the loss of equipment and data or to appropriately recover data. Without a disaster recovery plan, the Authority could lose important financial and other data and suffer a serious interruption to operations, such as not being able to process checks to pay vendors or employees or determine the status of rental payments receivable.

What Do We Recommend?

The Board should:

1. Adopt written IT policies and procedures to address acceptable computer use, individual access rights, password security management and disaster recovery.
2. Periodically review and update all IT policies and procedures to reflect changes in technology and the Authority's computing environment. Verify that IT back-up procedures are functioning properly.
3. Provide security awareness training to personnel who use IT resources.

Authority officials should:

4. Remove the access rights for the six network users who have left the Authority and ensure that all future users who leave employment have their access rights removed.
5. Secure the Authority's server to protect it from intentional or unintentional harm, loss or impairment.
6. Develop and maintain a complete, comprehensive software inventory or all software owned including the total number of licenses for each.
7. Monitor computer use to ensure all software is used for an appropriate business purpose.
8. Assign unique user accounts to employees and ensure that they are only provided with the access rights required to perform their job functions.

Appendix A: Response From Authority Officials

Newark HOUSING AUTHORITY

200 Driving Park Circle, PO Box 108
Newark, NY 14513-0108
(315) 331-1574
FAX (315) 331-0972
www.newarknyhousing.org

MEMBERS
ALAN VISINGARD
JANICE RISING
CHRIS THAYER
TONYA FINN
HELEN BLANDINO
BRUCE DECOOK
MARCIA PLAIN-OLIVERA

MARIE WASMAN
Executive Director
MATTHEW R. ST. MARTIN, ESQ
Counsel

March 26, 2018

Edward V. Grant, Jr., Chief Examiner
Division of Local Government and School Accountability
The Powers Building
16 West Main St., Suite 522
Rochester, NY 14614-1608

Re: Newark Housing Authority
Information Technology
2017M-282

Dear Chief Examiner Grant:

The Newark Housing Authority agrees with the findings in the audit report number 2017M-282.

The majority of the findings have been corrected to date. The balance will be corrected by the time we forward our corrective action plan, which will be forwarded before our 90 days expire.

Sincerely,

NEWARK HOUSING AUTHORITY

Marie Wasman
Executive Director

Alan Visingard
Chairman of the Board

Appendix B: Audit Methodology and Standards

We conducted this audit pursuant to Article X, Section 5 of the State Constitution. To achieve the audit objective and obtain valid audit evidence, our audit procedures included the following:

- We obtained and reviewed the Authority's IT policies and procedures.
- We interviewed Authority officials and the IT consultant to understand the IT environment and internal controls.
- We ran a specialized computer audit tool on the server and all 11 operational Authority computers. We used the tool to identify installed software, local account password settings and user account configurations.
- We reviewed Internet web history on the server and all 11 operational computers to determine if the computers were being used for appropriate business activities.
- We compared system users to payroll reports to determine whether users were currently employed by the Authority.

Our audit also examined the adequacy of certain IT controls. Given the sensitivity of some of this information, we did not discuss the results in this report, but instead communicated them confidentially to Authority officials.

We conducted this performance audit in accordance with GAGAS (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 objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Good management practices dictate that the Board has the responsibility to initiate corrective action. As such, the Board should prepare a plan of action that addresses the recommendations in this report and forward the plan to our office within 90 days.

Appendix C: Resources and Services

Regional Office Directory
www.osc.state.ny.us/localgov/regional_directory.pdf

Cost-Saving Ideas – Resources, advice and assistance on cost-saving ideas
www.osc.state.ny.us/localgov/costsavings/index.htm

Fiscal Stress Monitoring – Resources for local government officials experiencing fiscal problems
www.osc.state.ny.us/localgov/fiscalmonitoring/index.htm

Local Government Management Guides – Series of publications that include technical information and suggested practices for local government management
www.osc.state.ny.us/localgov/pubs/listacctg.htm#lgmg

Planning and Budgeting Guides – Resources for developing multiyear financial, capital, strategic and other plans
www.osc.state.ny.us/localgov/planbudget/index.htm

Protecting Sensitive Data and Other Local Government Assets – A non-technical cybersecurity guide for local government leaders
www.osc.state.ny.us/localgov/lgli/pdf/cybersecurityguide.pdf

Required Reporting – Information and resources for reports and forms that are filed with the Office of the State Comptroller
www.osc.state.ny.us/localgov/finreporting/index.htm

Research Reports/Publications – Reports on major policy issues facing local governments and State policy-makers
www.osc.state.ny.us/localgov/researchpubs/index.htm

Training – Resources for local government officials on in-person and online training opportunities on a wide range of topics
www.osc.state.ny.us/localgov/academy/index.htm

Contact

Office of the New York State Comptroller
Division of Local Government and School Accountability
110 State Street, 12th Floor, Albany, New York 12236

Tel: (518) 474-4037 • Fax: (518) 486-6479 • Email: localgov@osc.ny.gov

www.osc.state.ny.us/localgov/index.htm

Local Government and School Accountability Help Line: (866) 321-8503

ROCHESTER REGIONAL OFFICE – Edward V. Grant Jr., Chief Examiner

The Powers Building • 16 West Main Street – Suite 522 • Rochester, New York 14614-1608

Tel: (585) 454-2460 • Fax: (585) 454-3545 • Email: Muni-Rochester@osc.state.ny.us

Serving: Cayuga, Chemung, Livingston, Monroe, Ontario, Schuyler, Seneca, Steuben, Wayne, Yates counties

Like us on Facebook at facebook.com/nyscomptroller
Follow us on Twitter @nyscomptroller