# ERIE COUNTY WATER AUTHORITY
INTEROFFICE MEMORANDUM

July 3, 2018

To: Governance Committee-Commissioners Schad and Carney

From: Robert J. Lichtenthal, Jr., Deputy Director

Subject: Corrective Action Plan for OSC Technology Audit 2016-2017

---

The Office of the New York State Comptroller (OSC) conducted an audit of the Authority to determine whether Authority officials adequately safeguarded and protected information technology (IT) assets, used in its business environment, against unauthorized use, access and loss. The audit period was from January 1, 2016 to October 6, 2017 with draft reports received in March, 2018 and a final report received in April, 2018. Attached is a copy of the final report issued after an exit conference with Authority staff and the Board Treasurer.

The Authority is required to file a plan of corrective action within 90 days from the issuance of the report. The report was issued May 4, 2018. Prior to this time I was tasked with developing a Plan of Corrective Action to address the key findings. Attached to this memo please find my draft recommended plan and the timeframes within it is to be accomplished.

**NYS OSC Finding #1**

Authority officials did not develop procedures for managing system and network access

**NYS OCS Recommendation:**

Authority Officials Should:

Develop and implement written procedures for managing System and network access that include periodically reviewing user access and disabling or deleting user accounts when access is no longer needed.

**ECWA Plan of Corrective Action:**

The Authority will develop comprehensive written procedures for managing system and network access by December 31, 2018.

**NYS OCS Finding #2**

Internet usage was not routinely monitored

**NYS OSC Recommendations:**

The Board should:

Work with Authority officials to review and update the computer use policy and then ensure the IT Manager includes the updated policy when providing cybersecurity training to all employees.

**ECWA Plan of Corrective Action:**

The Authority will establish an IT Department Operating Procedure for routine monitoring of internet usage by December 31, 2018.

**NYS OSC Finding #3**

The Authority does not provide adequate cybersecurity training to employees.

**NYS OSC Recommendations:**

Ensure that cybersecurity training is provided periodically to all employees to address current and emerging risks.

**ECWA Plan of Corrective Action:**

The Authority will develop and implement an initial and on-going program of Cybersecurity Training for employees by December 31, 2018.

DIVISION OF LOCAL GOVERNMENT AND SCHOOL ACCOUNTABILITY

REPORT OF EXAMINATION | 2018M-9

# Erie County Water Authority

## Information Technology

MAY 2018


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

# Contents

# Report Highlights

**Erie County Water Authority**

## Audit Objective

Determine whether Authority officials adequately safeguarded and protected information technology (IT) assets, used in its business environment,[1] against unauthorized use, access and loss.

## Key Findings

- The Authority has 696 network user accounts that have not been used in the last six months, with 75 accounts last logon being over four years prior and 377 network user accounts that have never been used.
- Five of 10 tested employees visited social media, shopping websites and personal email which could expose the network to virus attacks or compromise systems and data.

In addition, sensitive IT control weaknesses were communicated confidentially to Authority officials.

## Key Recommendations

- Evaluate all existing network user accounts, disable or remove any deemed unnecessary and ensure these accounts are periodically reviewed for necessity and appropriateness.
- Review the Internet usage log to ensure compliance with the computer use policy.
- Address the IT recommendations communicated confidentially.

Authority officials agreed with our recommendations and indicated they planned to initiate corrective action.

## Background

The Erie County Water Authority (Authority) is a public benefit corporation established in 1949, providing water supply to approximately 550,000 customers across Western New York. The Authority is governed by three Board members, appointed by the Erie County Legislature and are responsible for the management and control of the Authority's operations. The Board appoints an Executive Director (Director) who is responsible, along with other administrative staff, for the Authority's day-to-day management under the Board's direction. The IT Manager[2] is responsible for day-to-day IT operations and reports to the Deputy Executive Director.

| Quick Facts | |
|---|---|
| Approximate Number of Employees | 250 |
| Approximate Number of Computers | 240 |

## Audit Period

January 1, 2016 – October 6, 2017[3]

1 We did not include any IT asset associated with the Authority's water supply operations.

2 During our audit period, the individual in this role had been appointed as "Acting IT Manager" on an interim basis.

3 For certain audit tests, we expanded our testing back to November 8, 2012.

# Information Technology

The Authority's IT system and the data stored in it are valuable resources. The Authority relies on its IT system for accessing the Internet, communicating by email and maintaining financial, personnel and customer records. If the IT system is compromised, the results could range from inconvenient to catastrophic and could require extensive effort and resources to evaluate and repair. While effective controls will not guarantee the safety of a computer system, the lack of effective controls significantly increases the risk that data, hardware and software systems may be lost or damaged by inappropriate access and use.

## What Are Effective Information Technology Controls?

Authority officials should develop comprehensive written procedures for managing system access that include periodic reviews of user access to ensure that user accounts are disabled or deleted when access is no longer needed. A computer use policy should be adopted that describes appropriate and inappropriate use of IT resources and compliance with that policy should be monitored by IT officials. Also, cybersecurity training should be provided to employees at least annually to address current risks identified by the IT community involving computer use and social media and other risks such as ransomware, malware and phishing.

## Authority Officials Did Not Develop Procedures for Managing System and Network Access

Authority officials did not develop comprehensive written procedures for managing system and network access. We were able to match all 241 accounts that access the Authority's administrative and business system (System) to current Authority and third-party users. However, due to the naming convention and lack of recorded detail for the 1,258 network user accounts, we were unable to effectively compare those accounts to user information. While officials may have additional information to identify user accounts, similar difficulties managing network access, and identifying and disabling or removing accounts that are no longer necessary could occur.

In addition, the Authority's network has 696 user accounts that have not been used in the last six months and of these, 75 user accounts were last used more than four years prior, while 377 have never been used. The IT Manager told us that, of the 696 network accounts, 221 are no longer necessary, including three with administrative network access. Although the unnecessary accounts we identified do not have direct access to the System, they could be used to disrupt legitimate access to the System or to gain unauthorized access to other resources on the network.

The IT Manager stated that he adds, modifies and deletes user accounts and permissions as requested through email, and that he and supervisors

occasionally review System and network access and permissions. However, Authority officials have not developed written procedures that address user access management. Further, officials do not regularly perform formal, comprehensive reviews of accounts and permissions.

Having inactive user accounts increases the risk for attacks on the Authority's networks. Additionally, because these user accounts are inactive, there is an increased risk that they are not being monitored, making it less likely that staff would notice these accounts being compromised or used for malicious purposes.

### Internet Usage Was Not Routinely Monitored

The Board has adopted a computer use policy. However, it was last updated in January 2012. We tested 10 employee's web histories and determined that five employees visited social media, shopping websites and personal email. Additionally, we noted a substantial amount of advertising content on three of these five computers, which could indicate adware.[4] While Authority officials stated that they monitor Internet usage on a case-by-case basis, the Authority does not routinely review Internet use to determine whether inappropriate use of the Authority's computers could expose the network to virus attacks or compromise systems and data, including key financial and confidential information. Furthermore, time spent by employees using Authority computers for personal reasons while they are supposed to be working represents lost productivity and Authority resources.

### The Authority Does Not Provide Adequate Cybersecurity Training to Employees

While the Authority provides brief IT training upon hire, there is no formal IT training on a regular basis. It is important to provide training to employees and to update the training material periodically to address current and emerging risks. Not providing cybersecurity training to employees increases the risk that users will not understand their responsibilities, putting the data and computer resources at greater risk for unauthorized access, misuse or abuse.

### What Do We Recommend?

Authority officials should:

1. Develop and implement written procedures for managing System and network access that include periodically reviewing user access and disabling or deleting user accounts when access is no longer needed.

4 Adware automatically displays or downloads advertising material.

The Board should:

2. Work with Authority officials to review and update the computer use policy and then ensure the IT Manager includes the updated policy when providing cybersecurity training to all employees.

The IT Manager should:

3. Review the Internet usage log to ensure compliance with the Authority's computer use policy.

4. Ensure that cybersecurity training is provided periodically to all employees to address current and emerging risks.

# Appendix A: Response From Authority Officials


**ERIE COUNTY WATER AUTHORITY**

3030 Union Road • Buffalo, New York 14227
716-684-1510 • FAX 716-684-3937


April 16, 2018

Jeffrey D. Mazula
Chief Examiner of Local Government and School Accountability
Office of the State Comptroller
295 Main Street, Room 1032
Buffalo, New York 14203

Dear Mr. Mazula:

On behalf of the Erie County Water Authority, I am writing you to acknowledge receipt of the Office of the State Comptroller's Draft Report of Examination of Information Technology for the Erie County Water Authority for the period from January 1, 2016 through October 1, 2017. In response to the findings and recommendations communicated through the draft report received on March 15, 2018 and discussed during the exit conference on March 22, 2018, the Authority will develop and implement a corrective action plan to address each potential concern.

The Authority would like to thank you and your staff for your recommendations and expertise. Our goal is to efficiently manage operations and provide transparency while providing all of our customers a plentiful supply of safe, high quality and affordable drinking water through a reliable infrastructure.

Sincerely,

Earl L. Jann
Executive Director

# Appendix B: Audit Methodology and Standards

We conducted this audit pursuant to Article V, Section 1 of the State Constitution and the State Comptroller's authority as set forth in 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 interviewed Authority officials and employees to obtain an understanding of the Authority's IT operations.
- We reviewed Authority records for any IT-related policies and procedures and reviewed those policies and procedures to obtain an understanding of the Authority's IT operations.
- We provided an audit script to the IT Manager on a universal serial bus (USB) drive to gather network user account data to identify accounts that had not been recently used.
- We obtained a list of active System accounts and a list of Authority employees. We compared the lists to identify any System account that is not associated with a current Authority employee.
- We judgmentally selected 10 computers with access to the administrative and business system. We analyzed the web-browsing histories to determine whether employees were complying with the Authority's computer use policy.

Our audit also examined the adequacy of certain IT controls. Because of 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.

Unless otherwise indicated in this report, samples for testing were selected based on professional judgment, as it was not the intent to project the results onto the entire population. Where applicable, information is presented concerning the value and/or size of the relevant population and the sample selected for examination.

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

---

**BUFFALO REGIONAL OFFICE** – Jeffrey D. Mazula, Chief Examiner

295 Main Street, Suite 1032 • Buffalo, New York 14203-2510

Tel (716) 847-3647 • Fax (716) 847-3643 • Email: Muni-Buffalo@osc.ny.gov

Serving: Allegany, Cattaraugus, Chautauqua, Erie, Genesee, Niagara, Orleans, Wyoming counties

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