DIVISION OF LOCAL GOVERNMENT AND SCHOOL ACCOUNTABILITY

REPORT OF EXAMINATION | 2021M-138

# Tully Central School District

## Network Access Controls

DECEMBER 2021

OFFICE OF THE NEW YORK STATE COMPTROLLER

Thomas P. DiNapoli, State Comptroller

# Contents

# Report Highlights

## Tully Central School District

## Audit Objective

Determine whether Tully Central School District (District) officials ensured network access controls over non-student user accounts were secure.

## Key Findings

District officials did not ensure that the District's network access controls over non-student user accounts were secure.

- Officials did not develop written procedures for granting, changing and revoking access rights.
- Officials did not regularly review enabled non-student user accounts to determine whether they were appropriate or needed. As a result, the District had 47 unneeded network user accounts, including 24 that were created for former employees or third-party consultants who no longer work for the District.
- Unneeded network user accounts can be potential entry points for attackers and could be used to inappropriately access the District's information technology systems.

Sensitive information technology (IT) control weaknesses were communicated confidentially to officials.

## Key Recommendations

- Develop and adhere to written procedures for granting, changing, revoking and reviewing network user account access.
- Disable unneeded network user accounts in a timely manner.

District officials agreed with our recommendations and indicated they would take corrective action.

## Background

The District is located in the Towns of Preble and Truxton in Cortland County and the Towns of Fabius, LaFayette, Onondaga, Otisco, Spafford and Tully in Onondaga County.

The seven-member Board of Education (Board) is responsible for managing and controlling the District's financial and educational affairs. The Superintendent of Schools (Superintendent) is the District's chief executive officer and is responsible for the District's administration.

The District's IT Director is responsible for managing the District's IT assets, including network security and user accounts.

| Quick Facts | |
|---|---|
| **Non-Student Network User Accounts** | 301 |
| **Number of Employees** | 182 |

## Audit Period

July 1, 2019 – February 11, 2021

# Network Access Controls

## Why Should Officials Manage Network User Accounts and Permissions?

District officials are responsible for restricting network user access to only those network resources and data needed for learning and to complete job duties and responsibilities. Network resources include those on networked computers, such as shared folders, and in certain applications, such as an email application. Restricting network user access helps ensure data and IT assets are protected from unauthorized use and/or modification.

Network user accounts identify specific individuals and accounts on networks, computers and applications, and provide user accountability by affiliating network user accounts with specific users and processes. Network user accounts are potential entry points for attackers because, if compromised, they could be used to inappropriately access and view data stored on the network.

A district should have written procedures for granting, changing and revoking user access to the network. To minimize the risk of unauthorized access, officials should actively manage network user accounts including their creation, use and dormancy, and regularly monitor them to ensure they are appropriate and authorized. When employees leave district employment, or when user accounts are otherwise no longer needed, officials should ensure that these accounts are disabled in a timely manner.

Generic accounts are not linked to individual users and may be needed for certain network services or applications to run properly. For example, generic accounts can be created and used for automated backup or testing processes, training purposes or generic email accounts, such as a service help desk account. Officials should routinely evaluate generic network user accounts and disable those that are not related to a current district or system need.

A district should have written procedures for granting, changing and revoking user access to the network.

Cybersecurity risks should be treated as any other hazard a school district may encounter along the way. District officials should identify the risks, reduce their vulnerabilities and plan for contingencies. This requires an investment of time and resources and a collaborative work environment among the superintendent, the board and the IT department.

## Officials Did Not Adequately Manage Network User Accounts and Access

District officials did not adequately manage network user accounts and access for the District’s network. Written procedures for granting, changing and revoking user access were not developed, and enabled user accounts were not regularly reviewed to ensure they were authorized and still needed. As a result, the District had unneeded accounts that had not been disabled, including accounts that went unused and/or were generic or shared by two or more users.

User Access Policy – The District has a written data access and security policy that requires officials to periodically grant, change and terminate user access rights to the networked computer system and to specific software applications. The policy also requires officials to ensure that users are given access based on, and necessary for, their job duties. However, this policy could be improved, as it does not include specific written procedures for granting, changing and terminating access rights and regularly reviewing enabled user accounts to ensure they are authorized and still needed.

The IT Director told us that principals or supervisors should email the help desk with requests to grant, modify or disable an employee's network user account. However, the IT Director stated he is not always notified in a timely manner when an employee no longer needs network access. Further, although the District has software to facilitate the monitoring of user accounts and can identify accounts that have never been logged into or that have gone unused for a set number of days, the IT Director stated he did not use this software because he lacked the time to configure it. He also told us the District did not have a process to regularly review enabled user accounts.

We reviewed all 301 non-student network user accounts and identified 47 accounts (16 percent) that were unneeded.

Unneeded Network User Accounts − We reviewed all 301 non-student network user accounts and identified 47 accounts (16 percent) that were unneeded. We found 24 of these accounts were assigned to former employees or third-party consultants who no longer worked for or provided services to the District. The remaining 23 unneeded accounts were generic or shared by two or more users. Of the 47 unneeded accounts, 11 had never been used to log in to the network. Further, 33 accounts had not been used in the last six months, including one account that last accessed the network in May 2006. The IT Director stated all 47 accounts were no longer needed and would be disabled.

Unneeded network user accounts can be potential entry points for attackers and could be used to inappropriately access and view personal, private and sensitive information (PPSI)[1] and compromise IT resources. Also, when a school district has many user accounts that must be managed and reviewed, unneeded user accounts may make it more difficult to manage network access.

District officials indicated the weaknesses identified in this report are, in part, the result of an insufficient amount of time and resources dedicated to cybersecurity. The reliance on technology, communication and interconnectivity has changed,

[1] PPSI is any information to which unauthorized access, disclosure, modification, destruction or use – or disruption of access or use – could have or cause a severe impact on critical functions, employees, customers, third parties or other individuals or entities.

and expanded the potential vulnerabilities and increased possible risk to operations. An appropriate investment should be made to evaluate the acceptable level of risk and then to facilitate the ongoing monitoring of that risk.

## What Do We Recommend?

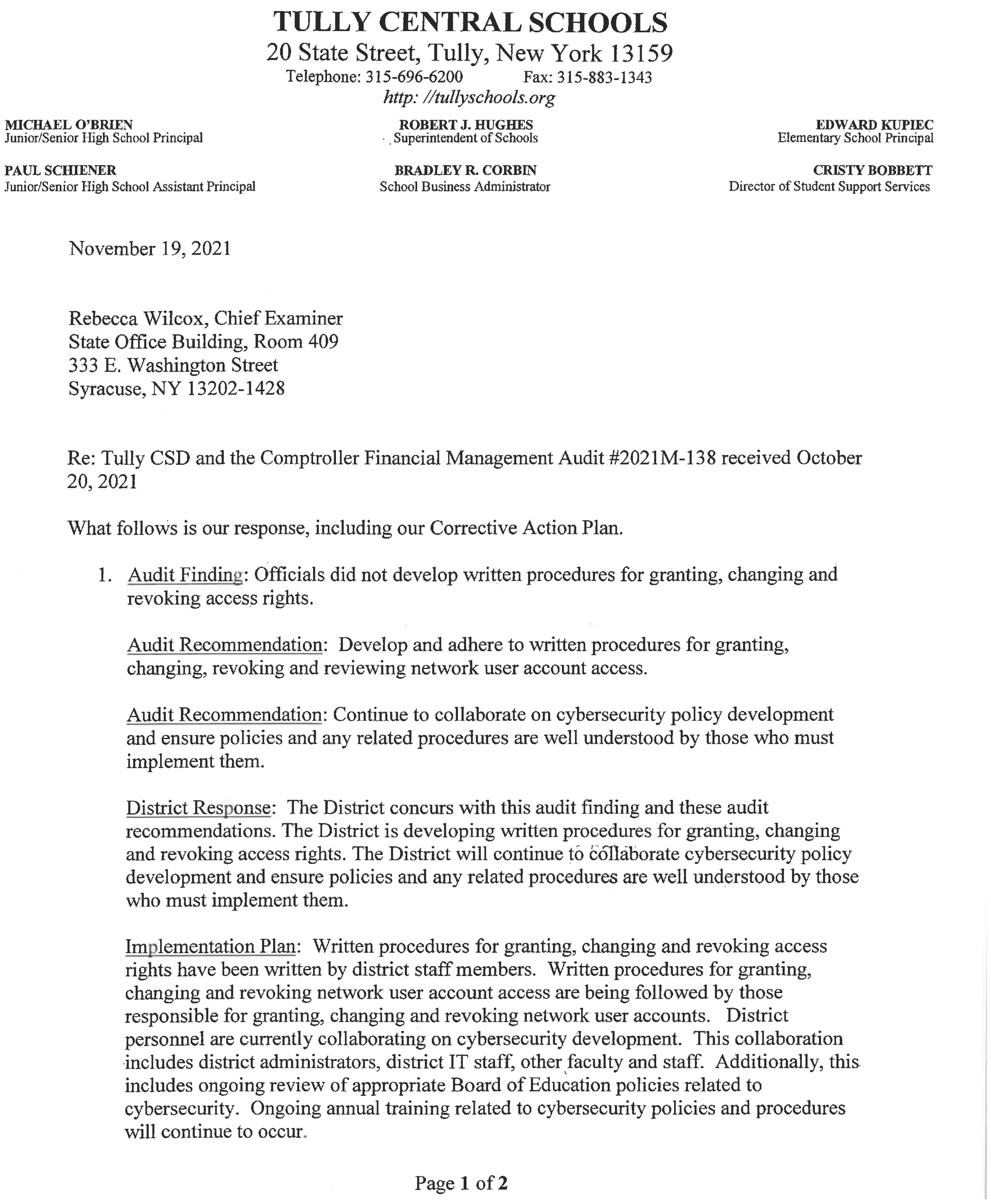
District officials and the IT Director should:

1. Develop and adhere to written procedures for granting, changing and revoking network user account access.
2. Disable network user accounts as soon as the users leave the District, and periodically evaluate existing network user accounts, including generic and shared accounts, and disable any deemed unneeded.
3. Continue to collaborate on cybersecurity policy development and ensure policies and any related procedures are well understood by those who must implement them.

The IT Director should:

4. Configure the software that identifies user accounts that have not been logged into and use this software to determine which unneeded accounts should be disabled.

# Appendix A: Response From District Officials



**TULLY CENTRAL SCHOOLS**
20 State Street, Tully, New York 13159
Telephone: 315-696-6200 Fax: 315-883-1343
*http: //tullyschools.org*

**MICHAEL O'BRIEN**
Junior/Senior High School Principal

**ROBERT J. HUGHES**
Superintendent of Schools

**EDWARD KUPIEC**
Elementary School Principal

**PAUL SCHIENER**
Junior/Senior High School Assistant Principal

**BRADLEY R. CORBIN**
School Business Administrator

**CRISTY BOBBETT**
Director of Student Support Services

November 19, 2021

Rebecca Wilcox, Chief Examiner
State Office Building, Room 409
333 E. Washington Street
Syracuse, NY 13202-1428

Re: Tully CSD and the Comptroller Financial Management Audit #2021M-138 received October 20, 2021

What follows is our response, including our Corrective Action Plan.

1. Audit Finding: Officials did not develop written procedures for granting, changing and revoking access rights.

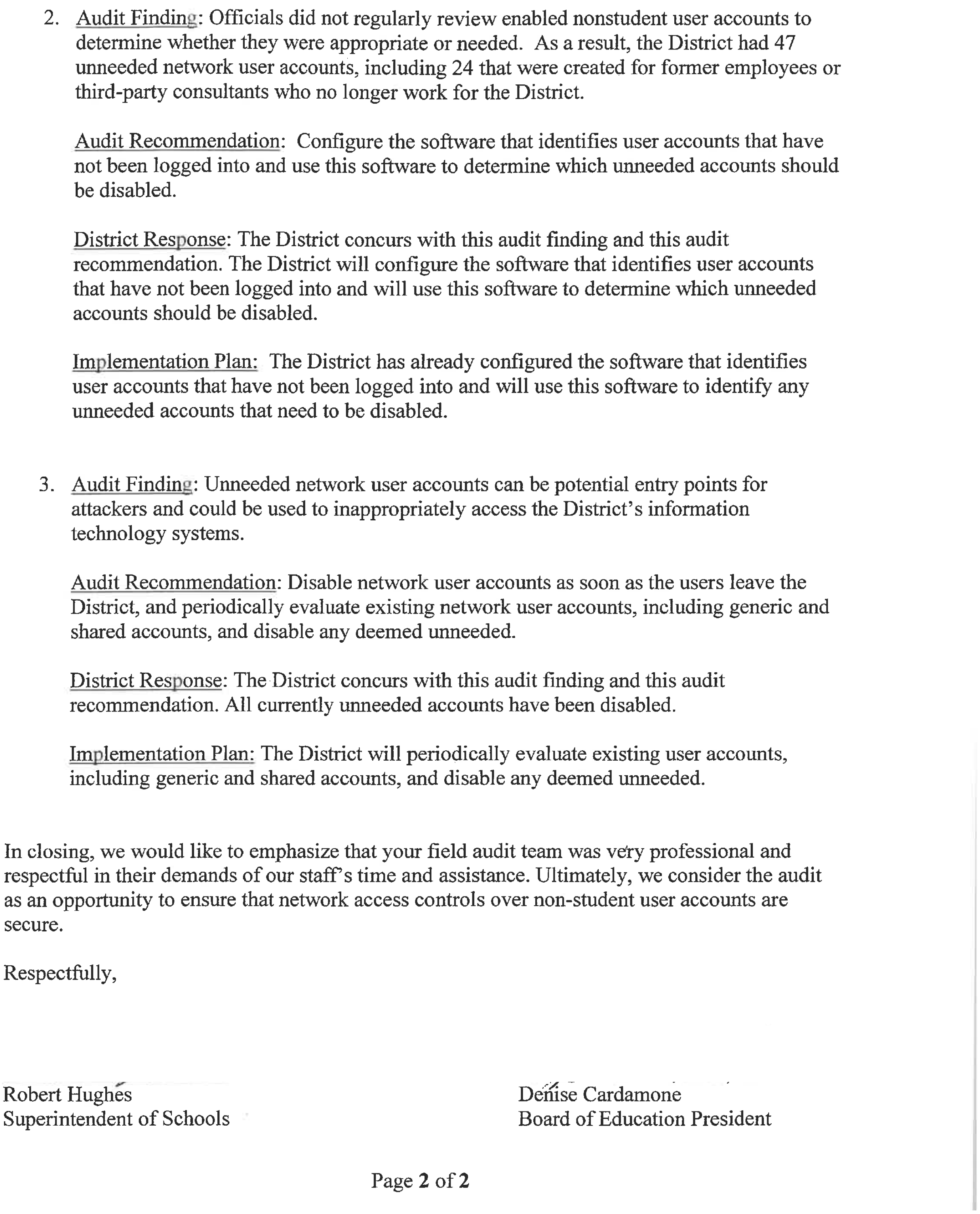
   Audit Recommendation: Develop and adhere to written procedures for granting, changing, revoking and reviewing network user account access.

   Audit Recommendation: Continue to collaborate on cybersecurity policy development and ensure policies and any related procedures are well understood by those who must implement them.

   District Response: The District concurs with this audit finding and these audit recommendations. The District is developing written procedures for granting, changing and revoking access rights. The District will continue to collaborate cybersecurity policy development and ensure policies and any related procedures are well understood by those who must implement them.

   Implementation Plan: Written procedures for granting, changing and revoking access rights have been written by district staff members. Written procedures for granting, changing and revoking network user account access are being followed by those responsible for granting, changing and revoking network user accounts. District personnel are currently collaborating on cybersecurity development. This collaboration includes district administrators, district IT staff, other faculty and staff. Additionally, this includes ongoing review of appropriate Board of Education policies related to cybersecurity. Ongoing annual training related to cybersecurity policies and procedures will continue to occur.

Page **1** of **2**



2. Audit Finding: Officials did not regularly review enabled nonstudent user accounts to determine whether they were appropriate or needed. As a result, the District had 47 unneeded network user accounts, including 24 that were created for former employees or third-party consultants who no longer work for the District.

   Audit Recommendation: Configure the software that identifies user accounts that have not been logged into and use this software to determine which unneeded accounts should be disabled.

   District Response: The District concurs with this audit finding and this audit recommendation. The District will configure the software that identifies user accounts that have not been logged into and will use this software to determine which unneeded accounts should be disabled.

   Implementation Plan: The District has already configured the software that identifies user accounts that have not been logged into and will use this software to identify any unneeded accounts that need to be disabled.

3. Audit Finding: Unneeded network user accounts can be potential entry points for attackers and could be used to inappropriately access the District's information technology systems.

   Audit Recommendation: Disable network user accounts as soon as the users leave the District, and periodically evaluate existing network user accounts, including generic and shared accounts, and disable any deemed unneeded.

   District Response: The District concurs with this audit finding and this audit recommendation. All currently unneeded accounts have been disabled.

   Implementation Plan: The District will periodically evaluate existing user accounts, including generic and shared accounts, and disable any deemed unneeded.

In closing, we would like to emphasize that your field audit team was very professional and respectful in their demands of our staff's time and assistance. Ultimately, we consider the audit as an opportunity to ensure that network access controls over non-student user accounts are secure.

Respectfully,

| | |
|---|---|
| Robert Hughes<br>Superintendent of Schools | Denise Cardamone<br>Board of Education President |

# 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 3 of the New York State General Municipal Law. To achieve the audit objective and obtain valid audit evidence, our audit procedures included the following:

- We reviewed the District's IT policies and procedures and interviewed District officials to gain an understanding of IT operations, specifically those related to the granting, modification and revocation of network user accounts and permissions.
- We ran a computerized audit script on the District's domain controller, which is the main server computer in the domain (network) that controls or manages all computers within the domain. We analyzed the data produced to assess network user accounts, permissions assigned to the accounts and the related security settings applied to the accounts. We compared the 301 non-student network accounts to the active employee list to identify accounts for former employees and/or other accounts that may be unneeded.
- We interviewed District officials regarding all possibly unneeded network accounts to determine the status of each account.

Our audit also examined the adequacy of certain information technology 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 District officials.

We conducted this performance audit in accordance with generally accepted government auditing standards (GAGAS). 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.

The Board has the responsibility to initiate corrective action. A written corrective action plan (CAP) that addresses the findings and recommendations in this report must be prepared and provided to our office within 90 days, pursuant to Section 35 of General Municipal Law, Section 2116-a (3)(c) of New York State Education Law and Section 170.12 of the Regulations of the Commissioner of Education. To the extent practicable, implementation of the CAP must begin by the end of the next fiscal year.  For more information on preparing and filing your CAP, please refer to our brochure, *Responding to an OSC Audit Report*, which you received with the draft audit report. The CAP should be posted on the District's website for public review.

# Appendix C: Resources and Services

**Regional Office Directory**
www.osc.state.ny.us/files/local-government/pdf/regional-directory.pdf

**Cost-Saving Ideas** – Resources, advice and assistance on cost-saving ideas
www.osc.state.ny.us/local-government/publications

**Fiscal Stress Monitoring** – Resources for local government officials experiencing fiscal problems
www.osc.state.ny.us/local-government/fiscal-monitoring

**Local Government Management Guides** – Series of publications that include technical information and suggested practices for local government management
www.osc.state.ny.us/local-government/publications

**Planning and Budgeting Guides** – Resources for developing multiyear financial, capital, strategic and other plans
www.osc.state.ny.us/local-government/resources/planning-resources

**Protecting Sensitive Data and Other Local Government Assets** – A non-technical cybersecurity guide for local government leaders
www.osc.state.ny.us/files/local-government/publications/pdf/cyber-security-guide.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/local-government/required-reporting

**Research Reports/Publications** – Reports on major policy issues facing local governments and State policy-makers
www.osc.state.ny.us/local-government/publications

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

## 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/local-government

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

**SYRACUSE REGIONAL OFFICE** – Rebecca Wilcox, Chief Examiner

State Office Building, Room 409 • 333 E. Washington Street • Syracuse, New York 13202-1428

Tel (315) 428-4192 • Fax (315) 426-2119 • Email: Muni-Syracuse@osc.ny.gov

Serving: Herkimer, Jefferson, Lewis, Madison, Oneida, Onondaga, Oswego, St. Lawrence counties

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