



Greece Public Library

Information Technology

Report of Examination

Period Covered:

January 1, 2016 – June 21, 2017

2017M-130



Thomas P. DiNapoli

Table of Contents

	Page
AUTHORITY LETTER	1
INTRODUCTION	2
Background	2
Objective	2
Scope and Methodology	2
Comments of Library Officials and Corrective Action	3
INFORMATION TECHNOLOGY	4
IT Policies	4
User Access	5
Hardware Inventory	5
Software Management	5
Disaster Recovery Plan	7
Recommendations	7
APPENDIX A Response From Library Officials	9
APPENDIX B Audit Methodology and Standards	12
APPENDIX C How to Obtain Additional Copies of the Report	13
APPENDIX D Local Regional Office Listing	14

State of New York Office of the State Comptroller

Division of Local Government and School Accountability

September 2017

Dear Library Officials:

A top priority of the Office of the State Comptroller is to help local government officials manage government resources efficiently and effectively and, by so doing, provide accountability for tax dollars spent to support government operations. The Comptroller oversees the fiscal affairs of local governments statewide, as well as compliance with relevant statutes and observance of good business practices. This fiscal oversight is accomplished, in part, through our audits, which identify opportunities for improving operations and Board governance. Audits also can identify strategies to reduce costs and to strengthen controls intended to safeguard local government assets.

Following is a report of our audit of the Greece Public Library, entitled Information Technology. This audit was conducted 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.

This audit's results and recommendations are resources for local government officials to use in effectively managing operations and in meeting the expectations of their constituents. If you have questions about this report, please feel free to contact the local regional office for your county, as listed at the end of this report.

Respectfully submitted,

*Office of the State Comptroller
Division of Local Government
and School Accountability*

Introduction

Background

The Greece Public Library (Library) is a municipal library located in the Town of Greece (Town) in Monroe County. The Library operates in a building adjacent to the Town hall and provides services to approximately 96,000 residents. The Library received its charter from the New York State Board of Regents in 1958 and is part of the Monroe County Library System (MCLS).¹ The Library lends books, magazines, movies and compact discs to those patrons with a library card. It also provides early literacy, teen and adult education programs and Wi-Fi service for patrons. In addition, the Library offers printing and copying services to patrons for a fee.

The Library is governed by a seven-member Board of Trustees (Board) appointed by the Town's governing body. The Board is primarily responsible for the general oversight of the Library's financial affairs and safeguarding information technology (IT) resources. The Board-appointed Library Director (Director) is responsible for day-to-day management, including managing staff. The Town's Finance Director is the Library's Treasurer. The Library receives IT support from a Library clerk (clerk), the Town's IT department and MCLS.

The Library's 2017 appropriations are approximately \$3.1 million, funded primarily with real property taxes, payments in lieu of taxes, state aid and revenue from printing service fees and fines collected on overdue materials.

Objective

The objective of our audit was to evaluate the Library's IT controls. Our audit addressed the following related question:

- Did Library officials adequately safeguard IT assets?

Scope and Methodology

We examined the Library's IT controls for the period January 1, 2016 through June 21, 2017. Because of the sensitivity of some of this information, we did not discuss the results in this report, but instead communicated them confidentially to Library officials.

We conducted our audit in accordance with generally accepted government auditing standards (GAGAS). More information on such

¹ MCLS is an association of 20 independent public libraries located in Monroe County and is chartered by the Board of Regents to provide services to libraries within the County. The MCLS administers a computer integrated library system and supports its member libraries by providing services such as maintaining computer databases of the libraries' inventory of materials on hand for loan, library patron borrowing histories, fines and fees paid, outstanding account balances and staff email.

standards and the methodology used in performing this audit are included in Appendix B of this report. 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 relevant population size and the sample selected for examination.

**Comments of Library
Officials and Corrective
Action**

The results of our audit and recommendations have been discussed with Library officials, and their comments, which appear in Appendix A, have been considered in preparing this report. Library officials agreed with our recommendations and indicated they planned to initiate corrective action.

The Board has the responsibility to initiate corrective action. A written corrective action plan (CAP) that addresses the findings and recommendations in this report should be prepared and forwarded to our office within 90 days, pursuant to Section 35 of General Municipal Law. 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. We encourage the Board to make this plan available for public review in the Director's office.

Information Technology

IT assets and computerized data are valuable resources that Library officials rely on for making financial decisions, processing transactions, keeping records and reporting to State and federal agencies. The potential consequences of an IT system failure range from inconvenient to severe. Accordingly, Library officials are responsible for establishing, designing and implementing comprehensive internal controls over the Library's IT system. The Board is responsible for adopting formal policies focused on protecting data and hardware from loss or misuse due to errors, malicious intent, accidents or disasters.

Because multiple parties have a role in the Library's IT functions, it is vital that the Board establish guidelines that clearly define the roles and responsibilities of each of the parties involved in providing IT services. The Board should periodically review and update these policies as necessary to reflect changes in technology or the Library's IT environment. In addition, Library officials should manage hardware and software to safeguard Library assets. A disaster recovery plan should be developed to prevent the loss of computerized data and to help Library personnel resume operations in the event of a disaster.

Library officials need to improve controls to ensure that Library IT assets are adequately safeguarded. The Board did not adopt any policies to protect its IT assets, establish written guidelines defining the roles and responsibilities of the Town's IT department and Library staff for the Library's IT environment or develop a disaster recovery plan. Additionally, Library officials did not have a comprehensive hardware inventory and can more effectively and efficiently manage software. As a result of these deficiencies, there is an increased risk that the Library's IT data and components may be lost or misused and that Library officials will be unable to resume operations in the event of a system failure.

IT Policies

IT security policies describe the tools and procedures to protect data and information systems, define appropriate user behavior, acceptable use and explain the consequences of policy violations. Therefore, it is essential the Board establish security policies for all IT assets and information. The Board should periodically review these policies, update them as needed and stipulate who is responsible for monitoring IT policies. New York State Technology Law requires local governments to establish an information breach notification policy. While libraries may not be subject to this law, it is in the Library's best interest to adopt and implement such a policy.

The Board has not adopted any IT policies, including those addressing acceptable use, password management, user accounts, access rights, data backups, hardware and software inventories, restricting personal use and connecting personally owned devices to Library computers, remote access or the sanitation and disposal of hardware and electronic media. The Board has also not adopted a breach notification policy. Additionally, there are no written guidelines to define the roles and responsibilities of the Town IT department and Library staff for the IT environment.

While IT policies do not guarantee the safety of the Library's IT assets or electronic information, the lack of policies significantly increases the risk that data from the Library's IT system may be lost or damaged by inappropriate access and use. Without formal policies that explicitly convey practices to safeguard data officials cannot ensure that employees are aware of their responsibilities.

User Access

Users should have access to the software and files they need to perform their job functions and not have access to other software and files. This can help to prevent unauthorized or unintentional changes to or deletion of data.

We found that all users had administrative rights on their computers. Acting as administrators, all employees had the ability to access all software and files on the computer system and the ability to download or install software that may not be needed to perform their duties and could put the system at risk of malware infection or intrusion.

Hardware Inventory

Library officials should maintain detailed up-to-date inventory records for all computer hardware. The information maintained should include a description of the item including make, model and serial number, name of the employee to whom the equipment is assigned (if applicable), the asset's physical location and relevant purchase or lease information including the acquisition date.

Library officials did not maintain comprehensive hardware inventory records. While officials were able to provide a list of hardware with serial numbers, it did not include the locations, names of users assigned or acquisition dates. Library officials cannot properly protect their IT resources if they are unaware which resources they have and where those resources are located. The lack of a comprehensive hardware inventory exposes these valuable assets to an increased risk of loss, theft or misuse.

Software Management

Managing software programs and licenses is essential to safeguarding Library assets and data. Therefore, Library officials must have an understanding of the software it owns, how it is used and the best

way to track user rights to ensure licensing compliance. Effectively managing software also includes ensuring that only appropriate software is installed to reduce the risk of unwanted consequences and unnecessary costs that could result from unauthorized software. This can be done, in part, by regularly reviewing computers to identify installed software and taking action to remove any unauthorized software.

A complete and comprehensive software inventory list is crucial to safeguard IT assets from potential unauthorized and unlicensed software being installed. The list should include all authorized software installed on Library computers, the number of copies currently in use and any pertinent licensing information, such as the total number of licenses for each software program.

A software license grants Library officials permission to use one or more copies of a software program in accordance with copyright law. It is essential Library officials regularly review all computers to ensure that the software installed is properly approved and licensed, particularly because staff has administrative rights that allow them to download and install software without prior permission or approval.

Library staff did not maintain a comprehensive software inventory of all Library software. Although officials provided us with a list of software and their total number of licenses, the list did not contain all Library software, indicate which computers each software program was installed on or the total number of copies of each software program installed.

Library officials have not developed formal written procedures for regularly reviewing computers. As a result, the clerk did not perform regular reviews of Library computers to determine whether installed software was appropriate or in compliance with licensing requirements. The regular review of software installed on computers is critical because staff have administrative rights that allow them to download and install software without prior permission or approval. As a result, the clerk and Library officials may not be aware of all installed software.

Further, the Director told us that staff have not had cybersecurity training. Therefore, there is an increased risk that staff may inadvertently download potentially dangerous software or malware and may not be aware of the importance of keeping up to date with software patches.

We reviewed the software installed on 10 computers² to determine whether the installed software was authorized, appropriate and licensed, if required. We found that approximately 1,015 installations³ on these computers were generally appropriate. However, we found that one

² See Appendix B for further details on our sample selection.

³ Includes preinstalled system software and components of larger software programs.

computer had one instance of malicious software. We identified 193 installations that required licensing. We reviewed licensing documentation, including purchase orders and invoices⁴ for these programs and found that the Library had an adequate number of licenses for the programs installed on these computers.

Without a comprehensive software inventory, it is unlikely that software patches necessary to address known security vulnerabilities will be applied on a timely basis, if at all. There is also an increased risk that inappropriate and potentially dangerous software is installed and goes undetected. Additionally, Library staff may inadvertently violate copyright laws by having more copies of software installed than licenses for a particular software, which could result in the Library incurring fines or penalties for installing unlicensed software.

Disaster Recovery Plan

A disaster recovery plan provides a framework for reconstructing vital operations to ensure the resumption of time-sensitive operations and services in the event of a disaster. Such disasters may include any sudden, catastrophic event (e.g., fire, computer virus, power outage or a deliberate or inadvertent employee action) that compromises the availability or integrity of the IT system and data. The plan should detail the precautions to minimize the effects of a disaster and enable the Town to maintain or quickly resume mission-critical functions. The plan should put a significant focus on disaster prevention and be distributed to all responsible parties, periodically tested and updated as needed.

The Board did not adopt a comprehensive disaster recovery plan to address potential disasters. The Director told us that the Library relies on the Town for its disaster recovery plan. However, the Town does not have a comprehensive disaster recovery plan. Further, officials would need to address the aspects of that plan, which are specific to Library operations. As a result, there is an increased risk that the Library's data could be lost or misused and that the Library will not be able to resume operations in the event of a system failure or disaster.

Recommendations

The Board should:

1. Adopt comprehensive IT policies that include acceptable use, password management, user accounts, access rights, backups, breach notification, hardware and software inventories, restricting personal use and connecting personally owned devices to Library computers and the sanitation and disposal of hardware and electronic media.

⁴ An effective and efficient method for purchasing and accounting for software licenses is through a purchase order system. A purchase order serves as the source document for vendor payment claims for various licenses obtained by the Library and provides a record of licenses on hand to avoid duplicate purchases.

2. Limit employees' access to only the software and data needed to perform their job duties.
3. Ensure that officials and employees receive adequate Internet security awareness training and training on the Library's IT policies.
4. Adopt a comprehensive disaster recovery plan and ensure that the plan is distributed to all essential personnel.

Library officials should:

5. Maintain complete, comprehensive hardware inventory records that detail the locations, assigned users and acquisition dates.
6. Maintain a complete, comprehensive software inventory list of all Library software, including the total number of licenses for each software, the computer on which each software program is installed and the number of copies of each software installed.
7. Formalize procedures to perform reviews of software installed on Library computers and compare these results to Library's software inventory records.

APPENDIX A
RESPONSE FROM LIBRARY OFFICIALS

The Library officials' response to this audit can be found on the following pages.

September 21, 2017

Via 1st Class Mail and E-Mail

Edward V. Grant, Jr., Chief Examiner
Office of the State Comptroller
The Powers Building
16 West Main Street, Suite 522
Rochester, New York 14614

Re: Response to Draft Report of Examination; 2017M-130

Dear Mr. Grant:

I am writing on behalf of the Town of Greece Public Library ("Library") in response to the findings and recommendations contained in the New York State Office of the Comptroller's draft Information Technology Report of Examination ("Draft Report").

As stated in the Draft Report, the Library is a municipal library governed by a seven-member board of trustees ("Board") that provides services to approximately 96,000 residents. The Library's mission is to engage, inspire and inform through community relevant learning opportunities. We execute this mission by offering loans of physical and digital library materials (586,000 loans in 2016), early literacy classes six days a week, reading incentive programs for all ages, comfortable and functional spaces for individual and group study, and public access computing and technology including WiFi, 3D printing, and scanning services. In 2016, more than 360,000 people visited the Library, 25,000 attended a program, and library computers were utilized 56,000 times.

On behalf of the entire Board, I would like to thank your office for the initial risk assessment you conducted of our Library operations and the thorough evaluation of the Library's information technology ("IT") controls. As detailed above, and as I believe was evident throughout this examination, the Library is an outstanding resource for residents that is operated with the highest level of professionalism and proficiency. As expected, we are pleased that during this approximately 8-month review process, your office found no instances of loss, theft or misuse of any Library IT assets and further found no evidence of any breach of Library IT security or unauthorized access to Library IT assets.

The Draft Report includes several recommendations for best practices to be considered by the Board and Library officials relating to IT policies, guidelines and procedures, employee access, and IT inventories. As the Board believes that the Library should constantly be looking to improve our operations whenever possible, I am pleased to report that, as of the date of this letter, the Board and Library administration have appropriately addressed and implemented each recommendation included in the Draft Report. As discussed during the exit conference, a more detailed report will be provided to your office specifying the corrective action that was taken to address and resolve each recommendation contained in the Draft Report.

The Library will continue to provide residents of the Town of Greece with the high level of service they have come to expect, and we again thank you for the thorough evaluation and recommendations to assist us in improving our IT-related policies and procedures.

Very truly yours,

Kevin M. Nasca
President
Greece Public Library Board of Trustees

APPENDIX B

AUDIT METHODOLOGY AND STANDARDS

To achieve our audit objective and obtain valid evidence, we performed the following procedures:

- We interviewed Library and Town officials and employees to gain an understanding of the IT environment.
- We reviewed Board minutes, the document of understanding with MCLS and computer hardware and software inventories.
- We used specialized audit software on a judgmental sample of ten computers to identify the software installed. We selected the two computers with access to the Library financial application, six staff computers and two patron computers. We reviewed the installed software to determine whether licenses were required. We also reviewed licensing documentation, such as purchase orders and invoices, to determine whether the Library maintained licenses for the software installed on each of these computers.

We conducted this performance audit in accordance with 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.

APPENDIX C

HOW TO OBTAIN ADDITIONAL COPIES OF THE REPORT

To obtain copies of this report, write or visit our web page:

Office of the State Comptroller
Public Information Office
110 State Street, 15th Floor
Albany, New York 12236
(518) 474-4015
<http://www.osc.state.ny.us/localgov/>

APPENDIX D
OFFICE OF THE STATE COMPTROLLER
DIVISION OF LOCAL GOVERNMENT
AND SCHOOL ACCOUNTABILITY

Andrew A. SanFilippo, Executive Deputy Comptroller
Gabriel F. Deyo, Deputy Comptroller
Tracey Hitchen Boyd, Assistant Comptroller

LOCAL REGIONAL OFFICE LISTING

BINGHAMTON REGIONAL OFFICE

H. Todd Eames, Chief Examiner
Office of the State Comptroller
State Office Building, Suite 1702
44 Hawley Street
Binghamton, New York 13901-4417
(607) 721-8306 Fax (607) 721-8313
Email: Muni-Binghamton@osc.state.ny.us

Serving: Broome, Chenango, Cortland, Delaware,
Osego, Schoharie, Sullivan, Tioga, Tompkins Counties

BUFFALO REGIONAL OFFICE

Jeffrey D. Mazula, Chief Examiner
Office of the State Comptroller
295 Main Street, Suite 1032
Buffalo, New York 14203-2510
(716) 847-3647 Fax (716) 847-3643
Email: Muni-Bufferalo@osc.state.ny.us

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

GLENS FALLS REGIONAL OFFICE

Jeffrey P. Leonard, Chief Examiner
Office of the State Comptroller
One Broad Street Plaza
Glens Falls, New York 12801-4396
(518) 793-0057 Fax (518) 793-5797
Email: Muni-GlensFalls@osc.state.ny.us

Serving: Albany, Clinton, Essex, Franklin,
Fulton, Hamilton, Montgomery, Rensselaer,
Saratoga, Schenectady, Warren, Washington Counties

HAUPPAUGE REGIONAL OFFICE

Ira McCracken, Chief Examiner
Office of the State Comptroller
NYS Office Building, Room 3A10
250 Veterans Memorial Highway
Hauppauge, New York 11788-5533
(631) 952-6534 Fax (631) 952-6530
Email: Muni-Hauppauge@osc.state.ny.us

Serving: Nassau and Suffolk Counties

NEWBURGH REGIONAL OFFICE

Tenneh Blamah, Chief Examiner
Office of the State Comptroller
33 Airport Center Drive, Suite 103
New Windsor, New York 12553-4725
(845) 567-0858 Fax (845) 567-0080
Email: Muni-Newburgh@osc.state.ny.us

Serving: Columbia, Dutchess, Greene, Orange,
Putnam, Rockland, Ulster, Westchester Counties

ROCHESTER REGIONAL OFFICE

Edward V. Grant, Jr., Chief Examiner
Office of the State Comptroller
The Powers Building
16 West Main Street, Suite 522
Rochester, New York 14614-1608
(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

SYRACUSE REGIONAL OFFICE

Rebecca Wilcox, Chief Examiner
Office of the State Comptroller
State Office Building, Room 409
333 E. Washington Street
Syracuse, New York 13202-1428
(315) 428-4192 Fax (315) 426-2119
Email: Muni-Syracuse@osc.state.ny.us

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

STATEWIDE AUDITS

Ann C. Singer, Chief Examiner
State Office Building, Suite 1702
44 Hawley Street
Binghamton, New York 13901-4417
(607) 721-8306 Fax (607) 721-8313