REPORT OF EXAMINATION | 2019M-170

Forestville Central School District

Information Technology

FEBRUARY 2020

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

Contents

Report Highlights

Forestville Central School District

Audit Objective

Determine whether personal, private and sensitive information (PPSI) on, or accessed through, the District's information technology (IT) system was properly safeguarded.

Key Findings

- District officials did not provide formalized IT security awareness training for individuals who used the District's IT assets.
- Personal Internet use was found on computers assigned to employees who routinely accessed PPSI.
- Network and application user accounts were not properly managed.

In addition, sensitive information technology control weaknesses were communicated confidentially to District officials.

Key Recommendations

- Provide periodic IT security awareness training.
- Develop and implement written administrative regulations to further define the District's acceptable use policy guidelines.
- Develop comprehensive written procedures for managing network and application user accounts.

District officials agreed with our recommendations and have initiated or indicated they planned to initiate corrective action.

Background

The Forestville Central School District (District) serves the Towns of Hanover, Sheridan, Villenova and Arkwright in Chautauqua County and the Town of Perrysburg in Cattaraugus County. The District is governed by an elected seven-member Board of Education (Board). The Board is responsible for the general management and control of the District's financial and educational affairs.

The Superintendent of Schools (Superintendent) is the District's chief executive officer and is responsible, along with other administrative staff, for the District's day-to-day management under the Board's direction.

The District's Director of Technology and Communications (Director) is responsible for managing the District's IT operations and reports to the Superintendent.

Quick Facts	
Student Enrollment	455
Employees	155
Total Network Accounts[a]	560
Nonstudent Network Accounts	171

a These included student, teacher, staff and generic accounts, which are used by network services and applications to run properly.

Audit Period

July 1, 2017 – July 11, 2019

Information Technology

The District relied on its IT assets for Internet access, email and for maintaining financial, personnel and student records and data, much of which contained PPSI.[1]

Why Should Officials Provide IT Security Awareness Training?

To minimize the risk of unauthorized access and misuse or loss of data and PPSI, District officials should provide periodic IT security awareness training. This training should explain the proper rules of behavior for using the Internet, IT systems, data and PPSI, and communicate related policies and procedures to all individuals using them and explain the consequences of policy violations. The training should center on emerging trends such as information theft, social engineering attacks[2] and computer viruses, and other types of malicious software, all of which may result in PPSI compromise or expose the District to ransomware attacks. Additionally, District officials should develop and also communicate written procedures for collecting, storing, classifying, accessing and disposing of PPSI.

Training programs should be directed at the specific audience (e.g., system users or administrators). The training should also cover key security concepts such as the dangers of Internet browsing and downloading files and programs from the Internet, requirements related to protecting PPSI and how to respond if an information security breach is detected.

Employees Were Not Provided With IT Security Awareness Training

During our audit period, the District did not provide formalized IT security awareness training to employees. Officials told us that employees were given updates and cybersecurity information through District emails and at staff meetings and provided us with examples of emails to review. However, this was not a sufficient substitute for organized IT security awareness training.

The IT cybersecurity community identifies people as the weakest link in the chain to secure data and IT systems. District officials cannot protect the confidentiality, integrity and availability of data and computer systems without ensuring that users, or those who manage IT, understand the IT security policies and procedures and their roles and responsibilities related to IT and data security. Without periodic, formal security awareness training, users may not understand their responsibilities and are more likely to be unaware of a situation that could

1 Personal, private and sensitive information (PPSI) is any information in 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.

2 Social engineering attacks are methods used to deceive users into revealing PPSI and other confidential or sensitive information.

compromise IT systems and assets. As a result, data and PPSI could be at a greater risk for unauthorized access, misuse or loss.

How Does an AUP Protect IT Assets and PPSI?

A school district should have a written acceptable use policy (AUP) that defines the procedures for computer, Internet and email use. The AUP should describe what constitutes appropriate and inappropriate use of IT resources, management's expectations concerning personal use of IT equipment and user privacy and consequences for violating the AUP. Monitoring compliance with the AUP involves regularly collecting, reviewing and analyzing system activity for indications of inappropriate or unusual activity and investigating and reporting such activity.

Internet browsing increases the likelihood that users will be exposed to malware that may compromise data confidentiality, integrity or availability. District officials can reduce the risks to PPSI and IT assets by routinely monitoring Internet usage and by configuring web-filtering software to block access to unacceptable websites and help limit access to websites that comply with the AUP.

The District's AUP indicates that staff will be provided training regarding the proper use of the computer system and that additional regulations will be developed to further define the guidelines in the AUP. Staff are required to sign the AUP and return it to the District office indicating that their use of the computer system will conform to the AUP's requirements. The AUP states that personal use of the computer system on District time or on District owned equipment is discouraged.

Officials Did Not Monitor Compliance With the AUP

We reviewed the Internet browsing histories on 12 computers assigned to eight employees[3] whose job duties required them to regularly access or have access to PPSI, or other confidential information such as the District's online banking activity and employee and student information, and found personal Internet use on 10 computers each assigned to one of each eight employees. This included personal shopping and banking, web searches for non-District related subjects, social media use and personal email use.

District officials were unaware of this activity because they did not routinely monitor employee Internet use. Also, while the AUP indicated that personal use was discouraged, it did not include consequences for violating this requirement. In addition, the AUP did not indicate that District officials should monitor personal

3 Four employees in our sample had two computers assigned to them. Refer to Appendix B for further information on our sample selection.

Internet use. The Director told us that because he was the only IT contact on staff, he was unable to spend time monitoring employee Internet use.

Officials also did not develop any written administrative regulations to "further define general guidelines of appropriate staff conduct and use as well as proscribed behavior," as required by the AUP. In addition, we found that the eight employees' files did not contain a signed AUP.

Internet browsing increases the likelihood of computer systems being exposed to malicious software that may compromise PPSI. As a result, the District's computer system and any PPSI it contains have a higher risk of exposure to damage and PPSI breach, loss or misuse.

Why Is it Important To Maintain an Inventory and Identify Users of PPSI?

Data classification is the process of identifying and categorizing data to help officials make informed decisions about how to properly protect it. Data classification includes scanning data repositories and organizing the data to determine what it is, where it is located and how to protect it.

District officials should classify District data to properly identify where PPSI is stored and how to adequately protect it. Classifying the PPSI data and users can help identify the type of security controls appropriate for safeguarding and disseminating the data. In addition, PPSI policies should include consequences or escalation procedures for noncompliance.

The District had several written policies that address protecting, inventorying and classifying PPSI and procedures to follow should there be a data breach or PPSI compromise. One policy identifies a list of information that the District considers PPSI, which includes personally identifiable information. These policies are disseminated to employees through the employee handbook annually and also are posted on the District's website.

PPSI Was Not Properly Maintained

The District uses its computer system to collect and store data received and produced from its operations, which includes PPSI and other confidential financial, student and employee data. Although a District policy indicated what type of information that the District considered PPSI, we found that the District did not classify or maintain an inventory of the District's PPSI data itself and where PPSI is stored in the computer system. Further, the District's policies did not identify the specific users of the District's PPSI.

While the PPSI-related policies were properly disseminated and made available to employees, officials did not ensure that employees understood them and how

they related to their duties because the policies were not addressed during formal District training events. Further, the policies did not include consequences or escalation procedures for noncompliance with PPSI policies.

The policies also indicated that employees with access to PPSI would be advised as to the requirements regarding the release of PPSI, according to applicable laws. However, the policies did not identify how employees would be advised of this information (e.g., during training).

The Director told us that the District did not maintain a PPSI inventory because it would be labor-intensive and cost-prohibitive. However, without a PPSI inventory, the District cannot ensure that all PPSI is properly accounted for and protected in the event of improper data changes or deletions, unauthorized system access and data breaches.

Why Should the District Properly Manage User Accounts?

Computer networks[4] can be accessed by network user accounts, and software applications can be accessed using an application user account. Both types of user accounts identify specific users. Network user accounts are managed centrally by a server computer and/or domain controller[5] and provide access to resources on a network. Application user accounts are managed centrally by an application server[6] and provide access to resources within the application.

To minimize the risk of unauthorized network and application access, District officials should actively manage network and software application user accounts, including their creation, use and dormancy, and regularly review them to ensure they are still needed. When employees leave District employment or transfer to another area, or when user accounts are no longer needed, officials should ensure that these accounts are disabled in a timely manner.

Because shared accounts are not assigned to a single user, officials may have difficulty managing these accounts and linking any suspicious activity to a specific user. To help ensure individual accountability, all users should have and use their own user account to gain access to a network and applications. If shared accounts are needed, officials should have procedures in place to monitor who uses the accounts and when they are used.

4 A group of two or more connected computers

5 A server is a computer equipped with specific programs that provide resources and data to other computers which are connected to the server. A domain controller is the main server computer in the domain (network) that controls or manages all computers within the domain.

6 An application server is a program on a server computer that handles all application operations between users and an organization's back-end applications or databases. The front-end is the user interface, typically web-based, where users input information and make information requests. The back-end is the application and database on the server that delivers information to users.

IT managers should set up user accounts with specific user permissions needed by each individual to perform their job functions. This ensures access to PPSI is restricted to only those individuals who are authorized to access it. Officials should review and approve user permissions before the IT manager configures user accounts with specific permissions, and this approval should be documented. In addition, the District requires users of the special education application to sign confidentiality agreements acknowledging that PPSI contained in the system must be properly safeguarded.

The District's policy states that the Superintendent, or designee, will periodically grant, change and terminate user access rights to the District's computer system and to specific software applications, which include the District's financial, special education and student information management applications.

Officials Did Not Adequately Manage User Accounts and Access

Former Employees and Consultants – During our review of network accounts, we found five unneeded network user accounts that were assigned to former employees or consultants. Three were last accessed between October 13, 2016 and October 30, 2018, and two were never used to log into the network. User accounts of former employees and consultants that have not been disabled or removed could potentially be used by those individuals or others for malicious purposes.

Shared Accounts – During our review of network accounts, we found 59 shared network user accounts that had varied purposes, ranging from administrative functions such as accounts used to set clocks, instructional purposes such as accounts used by substitute teachers to access curriculum information and accounts used to access servers and configure web filtering settings.

Of the 59, District officials told us 14 were unnecessary and the remaining 45 were necessary. However, because there was such a large number of necessary shared accounts, officials could have difficulty managing them and tracing suspicious activity to a specific user. For example, of the 59 accounts, we found that 34 had never been used and five had not been used in the last six months.

In addition, officials did not have procedures in place to monitor who used the needed shared accounts. With such a large number of necessary shared accounts, it may not always be clear who uses the accounts and whether their access is still needed. As a result, the District has a greater risk that PPSI could be changed intentionally or unintentionally or used inappropriately and officials would not be able to identify who performed the unauthorized activities.

Software Application User Accounts – We reviewed user permissions of all 100 application user accounts for the District's student information management

software application, 10 user accounts for the special education application and three user accounts for the financial application.[7] All three applications contained PPSI and required network access, and we found that user permissions were properly set based on job function and did not appear excessive.

However, officials could not provide us with documented evidence to indicate that the Superintendent or his designee approved permissions for the student information management software application or the special education application. In addition, 47 users had access to the special education application and were required to sign confidentiality agreements. We reviewed the 10 agreements of the individuals' whose user accounts were selected for review and found that four were not signed. The Special Education Director's secretary told us she forgot to ensure the individuals signed the agreements.

User Access Policy – The District has an access approval policy that requires officials to "periodically grant, change, and terminate user access rights to the overall networked computer system and to specific software applications and ensure that users are given access based on, and necessary for, their job duties." However, this policy could be improved because it does not include specific written procedures for revoking access rights and regularly reviewing enabled user accounts.

Because the District did not have adequate procedures for revoking access rights and officials did not regularly review enabled user accounts, the active accounts of former employees and consultants and unneeded shared accounts went unnoticed until our audit. In addition, because the District's network had unused, unneeded active user accounts, it had a greater risk that these accounts could have been used as entry points for attackers to access PPSI and compromise IT resources.

What Do We Recommend?

The Board should:

1. Provide, or coordinate the provision of, periodic IT security awareness training to employees who use District IT resources.
2. Ensure District officials monitor and enforce employee compliance with District policies, including policies related to the use of and access to the computer system, PPSI and other sensitive data.
3. Amend the AUP to include consequences for noncompliance with the policy and require officials to monitor personal Internet use.

7 Refer to Appendix B for further information on our sample selection.

4. Amend District PPSI policies to ensure they require identifying specific users of the District's PPSI, include consequences or escalation procedures for noncompliance with the PPSI policies and identify how employees would be advised as to the requirements regarding the release of PPSI, according to applicable laws.

5. Ensure the Superintendent or his designee documents their approval of user permissions granted to IT users.

6. Consider amending the user access policy to include specific written procedures for revoking access rights and require officials to regularly review enabled user accounts.

District officials should:

7. Develop, disseminate and enforce written administrative regulations to supplement the District's AUP.

8. Monitor employee Internet use to ensure compliance with the AUP.

9. Ensure all IT users sign the AUP.

10. Develop a PPSI inventory by classifying all District data and identifying where it is stored in the computer system and who uses it. Also, periodically review and update the inventory.

11. Provide formal District training events that address the District's PPSI policies to users who routinely access PPSI.

12. Immediately disable network user accounts of former employees and consultants as soon as they leave District employment and routinely review network user accounts and disable those that are no longer needed.

13. Restrict the use of shared network user accounts and develop procedures to monitor who uses these accounts.

14. Ensure that all users who have access to the special education application sign confidentiality agreements.

15. Develop comprehensive written procedures for granting, changing and revoking network and user application accounts.

Appendix A: Response From District Officials

FORESTVILLE CENTRAL SCHOOL DISTRICT

12 Water Street
Forestville, New York14062

February 4, 2020

Jeffrey D. Mazula, Chief Examiner
295 Main Street
Suite 1032
Buffalo, New York 142032510

To Whom It May Concern:

This letter is an acknowledgement that the New York State Comptroller's Office conducted an extensive Information Technology Audit of Forestville Central School District's Information Technology hardware, software and operating systems including but not limited to internet usage, security and data storage. The Forestville Central School District is in receipt of the Draft Audit Report for the period July 1, 2017 through June 30, 2019. Please accept this letter as the District's response to the audit, as pursuant to General Municipal and NYS Education Law.

On behalf of the Board of Education and administration, we would first like to thank the local staff of the Comptroller's Office for their professionalism while conducting the audit. The auditors were courteous throughout the process and actively listened as they engaged with district faculty and staff. The District is thankful for the opportunity to receive valuable feedback to improve our policies and practices related to information security and privacy measures.

We agree with the findings of the audit process. We agree that the facts relied upon in preparing the findings are accurate and complete. We agree with the recommendations provided in the draft report. We will soon prepare our Corrective Action Plan and will submit It after review and approval by the Board of Education.

The District has already complied with the majority of recommendations in the Audit as suggested by the Examiner in Chief. The district will continue to improve on providing its users, employees and community a fundamentally safe, sound and beneficial educational IT environment.

In closing, I would like to thank the field staff of the Comptroller's Office for their professionalism and assistance throughout the review. If you have any questions regarding our response, you are encouraged to contact me.

Respectfully submitted,

Renee Garrett

Renee Garrett
Superintendent of Schools

Superintendent's Office (716) 965-6539 Fax (716) 965-2786
Business Office (716) 965-6540 Fax (716) 965-2117
Elementary Office (716) 965-2742 Fax (716) 965-2265
High School Office (716) 965-2711 Fax (716) 965-2102
The Forestville Central School District is an Equal Opportunity Employer

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 interviewed District officials and reviewed Board policies, regulations, meeting minutes and District administrative procedures relating to IT operations and assets. We did this to obtain an understanding of the IT environment and assess the adequacy of the District's IT policies and procedures regarding IT security awareness training, AUP compliance and enforcement, PPSI inventory classification and network and application user account management.
- We interviewed District officials and reviewed IT security update emails sent to employees by the Director to determine whether employees received periodic and organized IT security awareness training.
- We reviewed eight employees' Internet use on the 12 computers assigned to them to evaluate whether their Internet use was in compliance with the AUP. We used our professional judgment to select the eight employees based on job titles that indicated duties likely to involve accessing student, staff and financial PPSI. We also examined their employee files to determine whether all eight had signed the AUP.
- We provided the Director with a computerized audit script to run on the District's domain controller. We analyzed each report generated by the script to identify network user accounts and security settings that indicated ineffective IT controls.
- We compared the District's employee master and payroll list reports to names of account users listed in the audit script report to determine whether all users with active network accounts were currently employed or contracted by the District.
- From various software permissions reports, we identified users who had administrative permissions to the financial, special education and student information management software applications and determined how user permissions in the applications were managed. We then examined the user permissions to determine whether access was appropriate based on job duties and whether PPSI was limited to as few employees as possible.
    - For all 100 user accounts on the student information management application, we reviewed their user permissions to determine whether access to PPSI was appropriately restricted.
    - For the special education application, we used our professional judgment to select five District employees and five non-District employees (10 total) from a total population of 47 special education application users to

determine whether access was appropriately restricted. We made our selection from the 31 users who had the lowest level of access to the application. To make the actual selection of five users from each group, we used a random number generator. We also examined their employee files in the Special Education office to determine whether all 10 had signed a confidentiality agreement.

- For the financial application, we used our professional judgement to select three District employees from a total population of 16 financial application users to determine whether access was appropriately restricted. We based our sample selection on the job titles of those who would not have needed access to PPSI in all modules of the application to fulfill their job duties.

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.

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.

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/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/pubs/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/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