REPORT OF EXAMINATION | 2019M-175

# DeRuyter Central School District

## Information Technology

DECEMBER 2019

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

# Contents

# Report Highlights

**DeRuyter Central School District**

## Audit Objective

Determine whether District officials ensured students' personal, private and sensitive information (PPSI) was adequately protected from unauthorized access, use and loss.

## Key Findings

District officials did not:

- Limit or monitor employees' personal Internet browsing and their use of social media on District computers.
- Provide IT security awareness training to employees.
- Restrict user permissions to the network and the student information system software application (SIS) based on job duties.
- Disable unneeded network and local user accounts.

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

## Key Recommendations

- Review and update the acceptable computer use policy and monitor employees' personal Internet browsing and use of social media.
- Provide formal IT security awareness training to employees.
- Evaluate network and SIS user permissions to ensure users only have the permissions needed for their job duties and disable any unneeded user accounts.

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

## Background

DeRuyter Central School District (District) serves the Towns of DeRuyter, Cazenovia, Georgetown and Nelson in Madison County, Lincklaen and Otselic in Chenango County, Fabius in Onondaga County and Cuyler in Cortland County.

The District is governed by a five-member Board of Education (Board) that is responsible for the general management and control of educational and financial affairs. The Superintendent of Schools (Superintendent) is the chief executive officer and is responsible, along with other administrative staff, for day-to-day management. The District's Technology Coordinator is responsible for managing the IT environment and resources.

| Quick Facts | |
|---|---|
| **Enrollment** | 359 |
| **Employees** | 192 |
| **Total Network Accounts** | 507 |
| **Desktop, Laptop and Tablet Computers** | 615 |

## Audit Period

July 1, 2017 – January 31, 2019

We expanded our audit period forward to March 26, 2019 to review IT data.

# Information Technology

The District relies on its IT assets for Internet access, email and for maintaining personnel and student records that may contain PPSI.[1] The District has an agreement with the Onondaga-Cortland-Madison Board of Cooperative Educational Services (OCM BOCES) for the Central New York Regional Information Center (CNYRIC) to provide IT services including offsite backup services, firewall configurations, virus protection and updates, remote server hosting and training and technical support for the SIS application.

The District's SIS contains extensive PPSI about students including social security numbers, medical information, custody and order of protection information and grades. Authorized users of the SIS include teachers, administrators, secretaries, guidance counselors, parents, students, a medical consultant, OCM BOCES and CNYRIC employees and the SIS vendor.

The District assigns user permissions to the SIS through 20 different user groups.[2] District employees, the medical consultant, OCM BOCES and CNYRIC employees and the SIS vendor represent a combined total of 118 SIS user accounts in 18 of the 20 groups.[3] The SIS and user computers are connected to the District network and access to network resources is managed by the Technology Coordinator.

## How Does an Acceptable Use Policy Safeguard PPSI?

A school district should have an acceptable computer use policy that defines procedures for computer, Internet and email use. The policy also should describe what constitutes appropriate and inappropriate use of IT resources and the board's expectations concerning personal use of IT equipment and user privacy.

Monitoring compliance with an acceptable use policy involves regularly collecting, reviewing and analyzing system activity for indications of inappropriate or unusual activity and investigating and reporting such activity. Officials should monitor and analyze activities for signs of possible violations or imminent threats of violations of acceptable use policies. Automated mechanisms may be used to perform this process and can help a district and its IT personnel routinely assess computer use, investigate possible policy violations and even recognize and prevent violation attempts.

---

1 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 (students), third parties, or other individuals or entities.

2 User groups are established in the SIS and user permissions are assigned to the groups. Therefore, all individuals in a group will have the same user permissions. These user groups include the superuser (IT personnel), administrator (school principals), counseling (guidance counselors), medical (school nurse), census (secretaries) and CNYRIC support (IT personnel) group.

3 Students and parents were excluded from our SIS testing, because we found their user permissions were appropriate.

Internet browsing increases the likelihood that users will be exposed to malicious software that may compromise data confidentiality, integrity or availability. District officials can reduce the risks to PPSI and IT assets by monitoring Internet usage and by configuring web filtering software to block access to inappropriate and/or unacceptable websites.

## The District's Acceptable Use Policy Was Inadequate

The Board adopted an acceptable use policy entitled Staff Use of Computerized Information Resources for computer, Internet and email use of officials and employees. The policy allowed for personal use of social media networks or social networking sites during school time on District-owned equipment, on a limited basis. However, the policy does not clearly define what is considered on a limited basis. In addition, officials did not adequately monitor employees' personal use. Further, the District's web filters[4] did not prevent employees from engaging in personal activities such as visiting social media, online shopping and playing games.

We reviewed the Internet browsing histories on 16 employee computers[5] and identified significant personal Internet use on 10 of these computers. Six computers showed use of online shopping, two computers showed continuous personal daily use of a social media website and two computers showed the users frequently played online games.

However, to protect District IT assets and PPSI, computers should be used for educational purposes and incidental personal use of computers should be kept to a minimum to prevent interference with an employee's duties.

Adopting a policy that allows personal Internet browsing and use of social media networks or social networking sites without clearly defined limitations and adequate monitoring significantly increases the risk that student PPSI, data, hardware and software may be lost or damaged by inappropriate use or access.

## Why Should the District Provide IT Security Awareness Training?

To minimize the risk of unauthorized access, misuse and loss of data and PPSI, officials should provide periodic IT security awareness training that explains the proper rules of behavior for using the Internet and IT systems and data and communicates related policies and procedures to all employees. The training

4 A web content filtering software program prevents access to pre-defined prohibited websites, typically by comparing a requested website address to a list of known bad websites.

5 See Appendix B for information on our sampling methodology.

should center on emerging trends such as information theft, social engineering attacks[6] and computer viruses and other types of malicious software which can compromise PPSI. Training programs should be directed at the specific audience (e.g., system users or administrators) and include everything attendees need to perform their jobs.

The training should also cover key security concepts such as the dangers of downloading files and programs from the Internet or portable devices, such as thumb drives; the importance of selecting strong passwords; requirements related to protecting PPSI; risks involved with using unsecured Wi-Fi connections; or how to respond if a virus or an information security breach is detected.

## IT Security Awareness Training Was Not Provided

District officials did not provide employees with IT security awareness training to help ensure they understood security measures to protect PPSI. Although, the Technology Coordinator sent out periodic emails about security risks as she was made aware of them, this was not a sufficient substitute for formal IT security awareness training.

The IT cybersecurity community identifies people as the weakest link in the chain to secure data and IT systems. 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 IT security awareness training users may not understand their responsibilities and are more likely to be unaware of situations that could compromise IT assets. As a result, data and PPSI could be at greater risk for unauthorized access, misuse or abuse.

## Why Should the District Have a Disaster Recovery Plan?

To minimize the risk of data loss or suffering a serious interruption of service, District officials should establish a formal written disaster recovery plan (plan). The plan should address the potential for sudden, unplanned catastrophic events (e.g., fire, computer virus or inadvertent employee action) that could compromise the network and the availability or integrity of a district's IT system and data, including its SIS and any PPSI contained therein.

6 Social engineering attacks are methods used to deceive users into revealing confidential or sensitive information.

Typically, a plan involves analyzing business processes, focusing on disaster prevention and identifying roles of key individuals and necessary precautions to take to maintain or quickly resume operations. Additionally, such a plan should include data backup procedures such as ensuring a backup is stored offsite in case the building is destroyed or inaccessible and periodic backup testing to ensure backups will function as expected.

### The District's Disaster Recovery Plan Did Not Address IT Issues

The Board did not develop a formal disaster recovery plan as it relates to the IT environment to describe how officials would respond to potential disasters.

District officials told us that the SIS data was backed up regularly and backups were stored offsite. However, because officials did not have a plan that was specific to its IT environment, in the event of a phishing or ransomware attack,[7] personnel had no guidance or plan to follow to restore or resume essential operations in a timely manner.

Without a comprehensive written plan, the District has an increased risk that it could lose important student information and other data and suffer serious interruption to operations, such as not being able to provide the required services to qualified students, access important student information (e.g., health or custody information) or process student grades.

### How Should Officials Manage and Monitor User Permissions and Accounts?

IT managers must grant appropriate user permissions to each individual needed to perform their job functions. This ensures access to PPSI is restricted to only those individuals who are authorized to access it. Also, officials should periodically monitor user permissions to ensure that employees have access to only those areas or data that they need for their job functions.

Audit logs or change reports maintain a record of activity or show changes made in a computer application. District officials should review these reports to monitor for unusual activity to help ensure that only appropriate changes are being made by authorized users. These reports provide a mechanism for individual accountability and for management to reconstruct events.

7 Phishing is sending deceptive email messages in an attempt to gather personal information or infect computer systems with malicious software. Ransomware is a type of malicious software that prevents users from accessing their computer systems or electronic data until a ransom payment is made; it often encrypts all data access to the user including that accessible on the network, computer and applications.

.

User accounts provide access to networks, user computers and the SIS and should be actively managed to minimize the risk of misuse. A district should have written procedures for granting, changing and disabling user accounts. To minimize the risk of unauthorized access, district officials should regularly review enabled network, local user and the SIS accounts to ensure they are still needed and disable unnecessary accounts and remove unneeded permissions as soon as there is no longer a need for them. If not properly managed, user accounts could be potential entry points for attackers because they could be used to inappropriately access and view PPSI on the network, user computers and in the SIS.

Generally, a designated administrator has oversight and control of a system or application with the ability to add new users and change users' passwords and permissions. A user with administrative permissions on the network can make system-wide changes, including installing programs of their own choosing and manipulating settings configured for security purposes. The compromise of an administrative account allows greater damage than with a lesser-privileged account because these accounts have full control over the network, user computers and software applications, such as the SIS.

Whenever administrative permissions are needed for an employee's job duties, officials must ensure that the employee has two user accounts, the administrative account and a lesser-privileged account to be used for nonadministrative tasks, such as accessing email and browsing the Internet. Accounts with unneeded administrative permissions should be disabled. This can help protect the network, computers and the SIS from being compromised if the employee encounters ransomware or another type of malicious software.

## Officials Did Not Adequately Manage or Monitor SIS User Permissions

SIS User Permissions – We reviewed user permissions for six groups comprising 52 users[8] who could add, edit and delete PPSI in the SIS. We interviewed 10 officials and employees to determine whether the 52 users' assigned groups granted permissions that were compatible with and appropriate for the users' job duties and found the following:

- District officials told us that only teachers were authorized to change grades. Teachers entered student grades in the SIS within a specific time period. After that period passes, if grade changes need to be made for reasons such as grading errors, the Superintendent or a principal could extend the period to allow the teacher to make changes. However, we found that 36 nonteacher users (all users in the administrator, superuser and counseling groups) also had user permissions to change student grades even though it was not their responsibility to do so.

8 Superuser group (four District employees, 16 OCM BOCES & CNYRIC and five vendor users), administrator group (four District employees and one OCM BOCES user), counseling group (six District employees), medical group (three District employees), census group (seven District employees and the medical consultant) and CNYRIC support group (five OCM BOCES and CNYRIC users).

- The guidance secretary told us she was responsible for adding and editing student information in the SIS including social security numbers, custody and order of protection information. However, we found that seven census group users, 25 superuser group users and five administrator group users had these permissions even though it was not within their job responsibility to add or change this information.
- The nurse, assigned to the medical group, was responsible for adding and modifying student medical information. However, there were two other users in the medical group and 30 users in the administrator and superuser groups with user permissions to add and edit medical information even though it is not their responsibility to do so.
- The principals, guidance counselors, school psychologist and their secretaries were responsible for managing students' individualized educational plans (IEPs). However, three administrator group users and two census group users had these permissions even though it was not their responsibility to add, modify or delete student IEPs.

Assume Identity/Account – The SIS has features that allow a user to assume another user's identity to view information without making modifications. It also allows users to assume another users' account, permitting the assumed account user to view and make modifications to information such as making grade changes.

These features are used by the CNYRIC personnel and support team for troubleshooting purposes. Because these features could allow an individual to view information or perform functions he or she could not with his or her own account, the ability to assume an account or identity should be limited to only those individuals who need it to perform their job duties.

During our review of user permissions, we found that all users in the administrator and counseling groups and four users in the superuser group had inappropriate user permissions to assume another user's identity. Four users in the superuser and census groups had inappropriate permissions to assume another user's account.

Audit Logs – District officials did not monitor user activity in the SIS to ensure that only authorized users could add, edit and delete SIS information, which contains student PPSI. Officials were unaware that change reports and audit logs were available for the SIS that would have allowed them to monitor unauthorized activities, such as unapproved grade changes.

We obtained an audit log for the 2017-18 school year from the CNYRIC and reviewed approximately 35,600 grade related records[9] in the log to determine whether any users in the administrator, superuser or counseling groups made grade changes with the unneeded user permissions they were granted in the system. The only user in these groups that made any grade changes was the guidance secretary, who made 233 changes without supporting documentation.

While officials were unaware that the guidance secretary made grade changes, she told us that teachers routinely asked her to make grade changes in person or occassionally through an email request. However, they did not provide her with documentation supporting the reason for the grade change.

Because District officials did not effectively manage and monitor SIS user permissions in accordance with job responsibilities, users had unneeded permissions that allowed unauthorized access to student PPSI. In addition, because officials did not periodically review SIS audit logs, they were unaware that the guidance secretary was making grade changes and may not detect inappropriate use of the SIS.

## Officials Did Not Adequately Manage User Accounts

District officials did not have written procedures for monitoring or disabling user accounts. When an employee is hired, the employee's supervisor or an administrator provides the Technology Coordinator with a form that requests that the user be given a user account for the network, a user computer and/or the SIS.

However, because there are no written procedures for revoking access, the Technology Coordinator relies on verbal requests from District officials to delete or disable a user account.

Because the District did not have formal procedures for monitoring or disabling user accounts, unneeded user accounts and accounts with unneeded administrative permissions went unnoticed until our audit. We reviewed 507 network user accounts and 15 computers with 39 local accounts and found the following:[10]

Network and Local Accounts – We found that four network accounts belonged to former OCM BOCES employees. The Technology Coordinator told us OCM BOCES did not notify the District when their employment at the BOCES ended, so their accounts were not disabled. User accounts of former employees that have not been disabled or removed could potentially be used by those individuals or others for malicious purposes.

9 The records include grade entries, grade changes and grade related comments.

10 Network user accounts are used to access computers and other resources on a network, and local user accounts are used to access files and software programs on a specific computer. See Appendix B for information on our sample selection.

Also, we found 18 network and 10 local accounts that were not needed. The Technology Coordinator disabled the network accounts when we questioned their need and told us she will disable the 10 local accounts. Officials must disable unnecessary accounts as soon as there is no longer a need for them.

Unnecessary Administrative Permissions – We found six network accounts had unnecessary administrative permissions to the network. These permissions were removed after we questioned the Technology Coordinator of their need.

Also, we found 112 staff and teachers' network accounts[11] had unnecessary administrative permissions to five of the 15 computers reviewed. The Technology Coordinator told us the five computers were initially set up based on an image[12] that granted all staff and teachers local administrative access for installing necessary software updates. While this may have facilitated the computer set-up process, the Technology Coordinator did not remove the extra user accounts from the computers when they were assigned to the primary users.

After we inquired about the administrative access, the Technology Coordinator told us that she removed local administrative permissions from all users except network administrators and the computer's primary user. In addition to these five primary users having local administrative permissions, we found that the primary users of eight of the other computers reviewed also had local administrative permissions.

The Technology Coordinator told us that it is her standard practice to assign primary users administrative permissions so they can install updates for software applications on their computers. However, it is critical to limit the ability to install software programs (e.g., to IT personnel only) to minimize the risk of unauthorized and malicious software. Therefore, only designated, authorized IT personnel should be responsible for software installations and updates. Further, we question whether users would need local administrative permissions on a regular basis to install software updates.

If administrative permissions are required for these users, at the very least, the users should have separate, lesser privileged accounts and use the administrative accounts only when needed. Limiting the use of administrative accounts significantly decreases the risk of computer issues from malware/ransomware or simple human error.

11 A total of 40 staff accounts and 72 teacher accounts were assigned to the computers through their respective account groups on the network.

12 Using an imaging process allows for the efficient setup of multiple similar computers. The imaging process involves replicating the contents of a computer's hard drive to new computers so that each computer is configured the same way and with the same software.

Because the District's network and user computers had 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. In addition, when employees have inappropriate administrative privileges within the network, user computers or software applications, they could make unauthorized changes that might not be detected. If a user is logged in with an account that has administrative permissions, an attacker could cause greater damage than with a lesser-privileged account.

## What Do We Recommend?

The Board should:

1. Review and update the acceptable use policy to clearly define limitations for Internet browsing and personal use of social networking sites.
2. Develop and adopt a formal disaster recovery plan that addresses the IT environment and ensure it is distributed to all responsible parties, periodically tested and updated as needed.

District officials should:

3. Clearly define users authorized to make grade changes and ensure that documentation is retained to show who authorized the grade change and the reason for the change.

The Technology Coordinator and District officials should:

4. Monitor compliance with the acceptable use policy and the use of personal Internet browsing and social media on a periodic basis.
5. Adjust web filter settings to help ensure computers are used for appropriate purposes only.
6. Provide formal IT security awareness training on an ongoing basis to all employees who use IT resources.
7. Regularly review user permissions granted to individuals with access to the network, computers and the SIS to determine whether they are appropriate and needed to perform their job duties and adjust and/or revoke excessive permissions that are deemed unnecessary.
8. Periodically review audit logs for unusual or unauthorized activity.
9. Develop written procedures for monitoring, disabling user accounts.

10. Disable the accounts of any users who are no longer employed at the OCM BOCES and any accounts deemed unneeded.

11. Provide separate user accounts with lesser-privileged permissions to employees to use for nonadministrative tasks.

12. Ensure only designated, authorized IT personnel install software and updates.

# Appendix A: Response From District Officials


**DeRuyter Central School**

***Home of the Rockets***

711 Railroad Street, DeRuyter, NY 13052

Phone: 315-852-3400 Fax: 315-852-9600

**Kimberly O'Brien**
Director of Curriculum and Instruction

**David M. Brown, Ed. D.**
Superintendent of Schools

**James Southard**
Business Administrator

**Stephen Rafferty**
6-12 Principal/Director of Special Education

**Jenny Valente**
K-5 Principal/Director of Special Education


December 4, 2019

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

Dear Ms. Wilcox:

The DeRuyter Central School District has reviewed the draft Information Technology Audit Report (2019M-175) completed by your office. This letter will comprise the district's Written Audit Response.

The district appreciates the opportunity that this audit provided to examine and better understand our Information Technology practices and procedures, as well as the opportunity to strengthen our technology security.

Upon review of the draft audit, the district is in general agreement with the report and findings. We are pleased to report that the district has already taken steps to implement many of your recommendations. The timeline for completing all of the recommendations will be provided in the Corrective Action Plan to be reviewed and approved by the Board of Education at their meeting in January 2020.

On behalf of the Board of Education and District Administration, I would like to thank the Office of the State Comptroller for the learning experience that this audit provided.

David M. Brown, Ed. D.
Superintendent of Schools

cc: Board of Education

# 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 and CNYRIC personnel and reviewed the District's IT policies to gain an understanding of its IT environment, internal controls and emergency response plan.
- We used our professional judgement to select a sample of computers assigned to 16 SIS application users (15 District employees and a CNYRIC employee) because their assigned user groups gave them access to add, delete and/or modify PPSI in the SIS. We reviewed their user account and group permissions and determined whether they were appropriate based on job functions and needed access to sensitive data.
- We reviewed the web history data on 16 computers to determine whether there was any personal, questionable or inappropriate Internet use. We used our professional judgement to select our sample, which was composed of the 15 computers from our previous sample and one additional District official's computer.
- We ran a computerized audit script on 16 computers (15 employee computers and the domain controller). We analyzed the data produced to assess network user accounts and security settings applied to those accounts. We reviewed these user accounts and compared them to the current employee list to identify inactive and unneeded accounts.

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 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 relevant population size 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 2116-1(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

**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