REPORT OF EXAMINATION | 2018M-169

Dansville Central School District

Information Technology and Non-instructional Employee Leave Benefits

JANUARY 2019

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

Contents

Report Highlights

Dansville Central School District

Audit Objectives

Determine whether:

- The Board and District officials ensured information technology (IT) assets were safeguarded.
- District officials accurately maintained leave records for non-instructional employees.

Key Findings

- The Board and District officials have not adopted adequate security policies and procedures to safeguard IT assets.
- District officials did not provide IT security awareness training for employees.
- As of February 27, 2018, leave balances for 31 of the 40 non-instructional employees tested (78 percent) were inaccurate.

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

Key Recommendations

- Adopt comprehensive IT security policies, procedures and plans to safeguard IT assets and data.
- Provide periodic IT security awareness training to personnel who use IT resources.
- Ensure that amounts earned for leave are granted in accordance with contracts and Board approval and that leave records are accurately maintained and up-to-date.
- Address the confidentially communicated IT recommendations.

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

Background

The Dansville Central School District (District) serves the Towns of North Dansville, Conesus, Groveland, Ossian, Sparta, West Sparta and Springwater in Livingston County and the Towns of Dansville and Wayland in Steuben County.

The District is governed by a seven member Board of Education (Board) responsible for the general management and control of financial and educational affairs. The Superintendent of Schools is the chief executive officer responsible for day-to-day management and administration.

The Director of Curriculum, Instruction and Computer Technology (Director) is responsible, along with the technology coordinator and computer network administrator for the overall management of IT infrastructure. The human resources clerk is responsible for recording leave time earned and used.

Quick Facts	
Students	1,630
Employees	330
Desktops, Laptops and Tablets	3,500

Audit Period

July 1, 2016 – July 27, 2018

Information Technology

IT systems and data are valuable resources. The District relies on its IT assets for Internet access, email and for maintaining financial, personnel and student records. If the IT assets are compromised, the results could range from inconvenient to catastrophic and could require extensive effort and resources to evaluate and repair. While effective controls will not guarantee the safety of a computer system, a lack of effective controls significantly increases the risk that data, hardware and software systems may be lost or damaged by inappropriate access and use. Wayne Finger Lakes Board of Cooperative Educational Services (BOCES) handles the District's internet filtering and firewall/intrusion detection.

What Policies and Procedures Should the Board Adopt to Safeguard IT Assets and Data?

IT security policies describe the tools and procedures to protect data and information systems, define appropriate user behavior and explain the consequences of policy violations. Therefore, it is essential for the board to establish security policies for all IT assets and information.

District officials should have acceptable computer use policies that define specific consequences for violations and address security awareness. Additionally, the board should establish computer policies that take into account people, processes and technology and communicate them throughout the district.[1] The board should periodically review these policies, update them as needed and stipulate who is responsible for monitoring IT policies.

The Board Did Not Adopt and Officials Did Not Enforce Adequate IT Security Policies

Acceptable use policies are not monitored or enforced.

While District officials have acceptable use policies for IT assets, they are not monitored or enforced. In addition, the policies do not define specific consequences for violations or address connecting personal mobile computing and storage devices to the network. Connecting personal devices to the network can create security vulnerabilities and allow inappropriate access to IT assets and data. Further, the staff acceptable use policy does not require cybersecurity training for employees.[2]

We reviewed the web browsing histories of 21 users on 14 computers.[3] We found questionable Internet use for 11 users on 10 computers, such as online shopping, use of personal email and visiting social networking, travel, news and entertainment websites and website searches for jobs and real estate.

1 Refer to our publication *Information Technology Governance* available at http://www.osc.state.ny.us/localgov/pubs/lgmg/itgovernance.pdf

2 Refer to "Why Should District Officials Provide IT Security Awareness Training?" section of report.

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

The Board has not adopted IT security policies addressing data classification and regulations addressing the protection of personal, private and sensitive information (PPSI).[4] Further, the Board has not adopted policies addressing password management, wireless security, remote access, online banking, user account management and access rights, sanitation and disposal of IT equipment, backup and disaster recovery. Officials offered no explanation for not having these policies in place and told us that they would start developing them.

While policies will not guarantee the safety of IT assets and data, a lack of appropriate policies significantly increases the risk that data, hardware and software may be lost or damaged by inappropriate use or access. Without formal policies that specify appropriate computer equipment use and practices to safeguard data, officials cannot ensure that employees are aware of their responsibilities.

Why Should District Officials Provide IT Security Awareness Training?

Computer users must be aware of security risks and trained in practices that reduce internal and external threats to IT systems and data. While IT policies tell computer users what to do, IT security awareness training helps them understand their roles and responsibilities and provides them with the skills to perform them. Such training should center on:

- Emerging trends in information theft and other social engineering reminders;
- Limiting the type of PPSI collected, accessed or displayed to that which is essential for the function being performed;
- Malicious software, virus protection and the dangers of downloading files and programs from the Internet;
- Password controls; and
- Restricting physical access to IT systems and resources which can help protect them from intentional or unintentional harm, loss or compromise.

Employees Are Not Provided IT Security Awareness Training

District officials did not provide users with IT security awareness training to help ensure they understand IT security measures. As a result, the District's IT assets and data are more vulnerable to loss and misuse. For example, during our review of IT assets, we found that some teachers' computers were left unattended and logged on. Because teachers were not informed of the risks associated with

4 Such as practices to safeguard PPSI when collecting, storing or transmitting information as required by the District's information security breach and notification policy.

leaving their computers unattended and logged in, unauthorized access to District data could occur.

Why Should the District Have a Disaster Recovery Plan?

A disaster recovery plan provides a framework for reconstructing vital operations to resume time-sensitive operations and services after a disaster. Disasters may include any sudden, catastrophic event[5] that compromises the availability or integrity of an IT system and data.

Typically, a disaster recovery plan includes an analysis of business processes and continuity needs, disaster prevention instructions, specific roles of key individuals and precautions needed to maintain or quickly resume operations. Additionally, a disaster recovery plan should include data backup procedures, such as ensuring a backup is stored off-site in case the building is destroyed or inaccessible, and periodic backup testing to ensure backups will function as expected.

The Disaster Recovery Plan Was Inadequate and Not Distributed or Tested

Although officials eventually provided us with a one-page disaster recovery plan, both the Director and IT staff were unsure of its existence when asked for it. The plan was inadequate because it did not designate alternate work locations and IT equipment or identify staff responsible for restoring critical applications and systems listed in the plan. In addition, the plan did not provide details on how often the plan should be tested or updated.

Consequently, in the event of a disaster or a phishing or ransomware attack,[6] personnel have little guidance on how to help minimize or prevent the loss of equipment and data or to appropriately recover data. Further, without a comprehensive plan, the District could lose important financial and other data and suffer a serious interruption to operations, such as not being able to process checks to pay vendors or employees or process student grades and State aid claims.

Why Should the District Maintain Accurate and Up-to-Date Hardware and Software Inventory Records?

Computer hardware and software management is of particular importance to larger entities such as school districts that have many different users who perform a variety of functions. Typically, districts have several software applications and

5 Such as a fire, computer virus or inadvertent employee action

6 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.

multiple licenses for each. Maintaining complete and comprehensive hardware and software inventory records is crucial in safeguarding IT assets from loss or theft, tracking the installation of unauthorized and unlicensed software on computers and avoiding fines for unlicensed software installations.

As a best practice, software additions or changes should be made by IT administration, to ensure that the software works well with the network and is for proper purposes and properly licensed. The software inventory record should include all district-owned software installed on computers and the number of copies and version currently in use.

The software inventory record should be used in conjunction with a comprehensive hardware inventory record, which details computer locations and users, and regular reviews of all district-owned computers to ensure that all IT assets are accounted for and installed software is properly approved and licensed. Maintaining complete and up-to-date hardware and software inventory records helps the board develop a formal IT replacement plan.

Hardware and Software Inventory Records Were Inaccurate and Outdated

The technology coordinator maintained a hardware inventory that included the device, model, serial number, assigned user, location and BOCES inventory tag numbers, when applicable. Our review of account and security settings disclosed several inconsistencies in the hardware inventory and errors, such as 25 computers that were not included in the inventory.

We selected 15 of the 312 laptop and desktop computers to determine where they were located and were able to locate all of them.[7] However, one computer, marked for disposal was located at the District Clerk's home because she used it while on sick leave and did not promptly return it when she returned to work. She subsequently returned it to the District for our testing. Because District officials did not maintain up-to-date hardware inventory records, there is an increased risk that IT assets may be lost, stolen or misused. Further, the Board's ability to develop a formalized IT replacement plan is hindered.

Additionally, officials did not maintain a comprehensive software and corresponding license inventory. Instead, the IT staff maintain a folder containing various files with software information. Rarely did this information identify which computer the software was installed on or the version installed. Further, officials told us that they have not performed an updated cost-benefit analysis of licensing needs since April 2008 to determine whether sufficient licenses were obtained for installations or if reductions could achieve cost savings. While we did not identify

7 Refer to Appendix B for information on our sampling methodology.

any malicious software installed on the 15 computers tested, we identified 15 unwanted software installations and several outdated and unsupported software programs because staff have administrative rights to install software and did not update these installations.

Without a complete and comprehensive software inventory, officials have no assurance that all installed software is appropriately licensed and for proper purposes. Furthermore, it is unlikely that software patches necessary to address known vulnerabilities will be applied on a timely basis, if at all. The Board adopted a new inventory policy on April 10, 2018 to address our concerns.

What Do We Recommend?

The Board should:

1. Adopt comprehensive IT security policies addressing password management, protection of personal, private, sensitive information, wireless technology, remote access, data classification, mobile computing and storage devices, sanitation and disposal of electronic media, user accounts and access rights, online banking and data backups.
2. Update the acceptable use policies to include consequences for violating the policy and provisions for IT security awareness training.
3. Periodically review and update all IT policies and procedures to reflect changes in technology and the District's computing environment and stipulate who is responsible for monitoring all IT policies.
4. Develop and adopt a comprehensive disaster recovery plan, including backup procedures and offsite storage.
5. Develop a formalized IT replacement plan.

District officials should:

6. Implement a process for monitoring Internet use and enforcing the acceptable use policies.
7. Provide periodic IT security awareness training to all personnel who use IT resources, including the importance of appropriate use.
8. Maintain accurate and up-to-date hardware and software inventories.

Non-instructional Employee Leave Benefits

How Should Leave Benefits Be Accounted for?

Accrued leave represents paid time off earned by employees. District officials should periodically verify the accuracy of employee leave records including leave time earned and used. Sufficient records should be kept to ensure employees accrue, use and receive pay for time off to which they are entitled. Procedures should ensure that accrued leave is earned and carried over from year-to-year in accordance with district policies and collective bargaining agreements (CBAs), leave used is properly deducted from the leave balances and any payments for unused leave made to employees upon leaving district employment are based on accurate records.

Accrued Leave Was Not Adequately Recorded and Monitored

The Board did not develop a policy or written procedures for maintaining leave records. The District employs 166 non-instructional employees, in 15 different employee groups, who receive leave benefits (e.g., vacation, sick and personal leave) based on the terms negotiated in each of four employee CBAs or the annual Board-approved management confidential resolution. However, the processes used to request, approve and record leave were inconsistent from one employee group to the next, which allowed for different processes within a single negotiating unit. Throughout our audit, employees, department heads and officials expressed their lack of assurance that accrued leave balances were accurate.

The human resources clerk (clerk) is responsible for entering leave earned and used into the computerized leave tracking system. However, we found that she did not accurately enter these transactions in a timely manner. This process was further complicated because employees submitted leave requests electronically through another computerized software program, via email and on paper forms and the two systems were not interfaced. While the employees' direct supervisor approved their leave requests, supervisors were unable to verify whether the employee has sufficient available leave balances.

As of February 27, 2018, leave balances for 31 of the 40 non-instructional employees tested (78 percent) were inaccurate[8] because the clerk did not properly process the leave requests. We reviewed 1,602 properly approved leave request transactions, of which 122 were not recorded and 14 were inaccurately recorded in the leave tracking system.

Our review of recorded leave used disclosed that 14 entries lacked adequate support, such as an approved leave request. Entries made by the clerk to record leave earned each year for eight employees did not agree with the applicable

8 Two of the nine employees with accurate balances were new employees with no leave requests during our audit period. See Appendix B for information on our sampling methodology.

CBA or Board resolution. Additionally, sick leave balances were understated by 39.63 days for eight employees and overstated by 52.26 days for 16 employees. Vacation leave balances were understated by 16.5 days for eight employees and overstated by 23.5 days for another eight employees. Further, personal leave balances were understated by .5 days for one employee and overstated by 6.5 days for six employees.

In addition to the immediate effect these inaccuracies have on employees, future employee leave payments upon leaving District employment could pose unnecessary costs for the District.

What Do We Recommend?

The Board should:

9. Develop a policy and written procedures standardizing a process for maintaining leave records and requests.

District officials should:

10. Ensure that leave earnings are granted per contract and Board approval and leave balance records are accurately maintained, correct and up-to-date.
11. Designate an independent individual to periodically review leave accrual records for accuracy.
12. Contact leave request vendor to set up the systems to directly interface.

Appendix A: Response From District Officials[9]

Dansville CENTRAL SCHOOLS DANSVILLE, NY

January 4, 2019

Edward V. Grant, Chief Examiner
Office of the State Comptroller
Division of Local Government and School Accountability
16 West Main Street, Suite 522
Rochester, NY 14614

Dear Mr. Grant,

Thank you for the opportunity to work with the Office of the New York State Comptroller on our 2018 audit of information technology and employee leave benefits.

The District's Management Response is enclosed. The response is structured in a manner that corresponds to your report.

We accept the report of findings and have made progress toward addressing deficiencies in IT security and the accounting of leave accrual. We're grateful for the professionalism of your office and we've learned and grown from our interactions with [redacted]

Sincerely,

Paul J. Alioto
Superintendent of Schools

DR. PAUL J. ALIOTO
Superintendent

284 Main Street
Dansville, New York 14437
Phone (585) 335-4000
Fax (585) 335-4002

ROGER K. PARULSKI
School Business Official

9 The District's response letter refers to an enclosure that supports the response letter. Because the District's response letter provides sufficient detail of its actions, we did not include the attachment in Appendix A.

Dansville Central School District

Management Response to the NYS Comptroller's Information Technology and Non-instructional Employee Leave Benefits 2018 Audit

Report Highlights

Audit Objectives

Determine whether:

The Board and District officials ensured information technology (IT) assets were safeguarded.

District officials accurately maintained leave records for non-instructional employees.

Key Findings

- The Board and District officials have not adopted adequate security policies and procedures to safeguard IT assets.
- District officials did not provide IT security awareness training for employees.
- As of February 27, 2018, leave balances for 31 of the 40 non-instructional employees tested (78 percent) were inaccurate.

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

Key Recommendations

- Adopt comprehensive IT security policies, procedures and plans to safeguard IT assets and data.
- Provide periodic IT security awareness training to personnel who use IT resources.
- Ensure that amount earned for leave are granted in accordance with contracts and Board approval and that leave records are accurately maintained and up-to-date.
- Address the confidentially communicated.IT recommendations.

Information Technology

IT systems and data are valuable resources. The District relies on its IT assets for Internet access, email and for maintaining financial, personnel and student records. If the IT assets are compromised, the results could range from inconvenient to catastrophic and could require extensive effort and resources to evaluate and repair. While effective controls will not guarantee the safety of a computer system, a lack of effective controls significantly increases the risk that data, hardware and software systems may be lost or damaged by inappropriate access and use. Wayne Finger Lake Board of Cooperative Educational Services (BOCES) handles the District's internet filtering and firewall/intrusion detection.

What Policies and Procedures Should the Board Adopt to Safeguard IT Assets and Data?

IT security policies describe the tools and procedures to protect data and information systems, define appropriate user behavior and explain the consequences of policy violations. Therefore, it is essential for the board to establish security policies for all IT assets and information.

District officials should have acceptable computer use policies that define specific consequences for violations and address security awareness. Additionally, the board should establish computer policies that take into account people, processes and technology and communicate them throughout the district.[1] The board should periodically review these policies, update them as needed and stipulate who is responsible for monitoring IT policies.

> ***Board Policy 8630 and corresponding regulations define acceptable use for students, employees and visitors. Upon each login, users must agree to follow the guidelines of acceptable use before they can access the district network.***
>
> ***8630 - R further stipulates:***
>
> > ***"All users of the district's computer network and equipment are required to comply with the district's policy and regulations governing the district's computer network. Failure to comply with the policy or regulation may result in disciplinary action as well as suspension and/or revocation of computer access privileges.***
> >
> > ***Any information pertaining to or implicating illegal activity will be reported to the proper authorities. Transmission of any material in violation of any federal, state and/or local law or regulation is prohibited. This includes, but is not limited to materials protected by copyright, threatening or obscene material or material protected by trade secret. Users must respect all intellectual and property rights and laws."***
>
> ***8630 - R will be updated to include guidance on and consequences for cyber-bullying.***

The Board Did Not Adopt and Officials Did Not Enforce Adequate IT Security Policies

While District officials have acceptable use policies for IT assets, they are not monitored or enforced. In addition, the policies do not define specific consequences for violations or address connecting personal mobile computing and storage devices to the network. Connecting personal devices to the network can create security vulnerabilities and allow inappropriate access to IT assets and data. Further, the staff acceptable use policy does not require cybersecurity training for employees.[2]

We reviewed the web browsing histories of 21 users on 14 computers.[3] We found questionable Internet use for 11 users on 10 computers, such as online shopping, use of personal email and visiting social networking, travel, news and entertainment websites and website searches for jobs and real estate.

The District will develop an IT Handbook for students and staff that will expand upon, explain and codify explicit IT security procedures. The handbook will further delineate possible consequences for violations.

The Board has not adopted IT security policies addressing data classification and regulations addressing the protection of personal, private and sensitive information (PPSI).[4] Further, the Board has not adopted policies addressing password management, wireless security, remote access, online banking, user account management and access rights, sanitation and disposal of IT equipment, backup and disaster recovery. Officials offered no explanation for not having these policies in place and told us that they would start developing them.

While policies will not guarantee the safety of IT assets and data, a lack of appropriate policies significantly increases the risk that data, hardware and software may be lost or damaged by inappropriate use or access. Without formal policies that specify appropriate computer equipment use and practices to safeguard data, officials cannot ensure that employees are aware of their responsibilities.

The District will develop an IT Operations Manual for the IT Dept. to address data classification and delineate steps for addressing the protection of personal, private and sensitive information, user account management and access rights as well as inventory and the disposal of IT equipment. In addition, the District will develop an IT Handbook for employees that will codify password management, wireless security and sound practice. The IT Dept. in collaboration with EduTech will review and update our Disaster Recovery Plan and clearly delineate responsibilities.

Employees Are Not Provided IT Security Awareness Training

District officials did not provide users with IT security awareness training to help ensure they

understand IT security measures. As a result, the District's IT assets and data are more vulnerable to loss and misuse. For example, during our review of IT assets, we found that some teachers computers were left unattended and logged on. Because teachers were not informed of the risks associated with leaving their computers unattended and logged in, unauthorized access to District data could occur.

Formal IT security training will be provided to all employees every other year and to all new employees through SafeSchools to complement the IT Handbook. IT security training modules to be provided are:

1. ***Browser Security Basics***
2. ***Compliance with the Children's Internet Protection Act***
3. ***Cyber Security***
4. ***Online Safety: What Every Educator Needs to Know***

The Disaster Recovery Plan Was Inadequate and Not Distributed or Tested

Although officials eventually provided us with a one-page disaster recovery plan, both the Director and IT staff were unsure of its existence when asked for it. The plan was inadequate because it did not designate alternate work locations and IT equipment or identify staff responsible for restoring critical applications and systems listed in the plan. In addition, the plan did not provide details on how often the plan should be tested or updated.

Consequently, in the event of a disaster or a phishing or ransomware attack,[6] personnel have little guidance on how to help minimize or prevent the loss of equipment and data or to appropriately recover data. Further, without a comprehensive plan, the District could lose important financial and other data and suffer a serious interruption to operations, such as not being able to process checks to pay vendors or employees or process student grades and State aid claims.

The District is consulting with the Genesee Valley / Wayne - Finger Lakes Educational Technology Service (EduTech) to review and update our disaster recovery plan to more clearly delineate responsibilities. The District will examine implementation feasibility and test annually upon plan completion. Data recovery will be tested.

Hardware and Software Inventory Records Were Inaccurate and Outdated

The technology coordinator maintained a hardware inventory that included the device, model, serial number, assigned user, location and BOCES inventory tag numbers, when applicable. Our review of account and security settings disclosed several inconsistencies in the hardware inventory and errors, such as 25 computers that were not included in the inventory.

We selected 15 of the 312 laptop and desktop computers to determine where they were located and were able to locate all of them.[7] However, one computer, marked for disposal was located at

the District Clerk's home because she used it while on sick leave and did not promptly return it when she returned to work. She subsequently returned it to the District for our testing. Because District officials did not maintain up-to-date hardware inventory records, there is an increased risk that IT assets may be lost, stolen or misused. Further, the Board's ability to develop a formalized IT replacement plan is hindered.

Additionally, officials did not maintain a comprehensive software and corresponding license inventory. Instead, the IT staff maintain a folder containing various files with software information. Rarely did this information identify which computer the software was installed on or the version installed. Further, officials told us that they have not performed an updated cost-benefit analysis of licensing needs since April 2008 to determine whether sufficient licenses were obtained for installations or if reductions could achieve cost savings. While we did not identify any malicious software installed on the 15 computers tested, we identified 15 unwanted software installations and several outdated and unsupported software programs because staff have administrative rights to install software and did not update these installations.

Without a complete and comprehensive software inventory, officials have no assurance that all installed software is appropriately licensed and for proper purposes. Furthermore, it is unlikely that software patches necessary to address known vulnerabilities will be applied on a timely basis, if at all. The Board adopted a new inventory policy on April 10, 2018 to address our concerns.

The District's hardware inventory is managed by the IT Dept. and updated with new and disposed IT equipment. The District will review and update the inventory annually and codify inventory procedures in the IT Handbook. The District will document the hardware replacement plan.

The District has installed [redacted] which will provide us with a Software inventory on the Windows Devices. IT will review reports from [redacted] annually. This too will be codified in IT Handbook.

What Do We Recommend?

The Board should:

1. Adopt comprehensive IT security policies addressing password management, protection of personal, private, sensitive information, wireless technology, remote access, data classification, mobile computing and storage devices, sanitation and disposal of electronic media, user accounts and access rights, online banking and data backups.

   The District will expand upon current data protection policies and regulations and develop an IT Operations Manual and an IT Handbook that will address

each of these issues.

2. Update the acceptable use policies to include consequences for violating the policy and provisions for IT security awareness training.

   The District AUP will be updated to reflect these changes and include consequences for violations. This will be communicated to all employees annually and to new staff at orientation.

3. Periodically review and update all IT policies and procedures to reflect changes in technology and the District's computing environment and stipulate who is responsible for monitoring all IT policies.

   IT will develop an IT Operations Manual that will codify IT policies and procedures and delineate responsibilities. This will be reviewed and updated annually.

4. Develop and adopt a comprehensive disaster recovery plan, including backup procedures and offsite storage.

   The District is consulting with the Genesee Valley / Wayne - Finger Lakes Educational Technology Service (EduTech) to review and update our disaster recovery plan to more clearly delineate responsibilities. The District will examine implementation feasibility and test annually upon plan completion. Data recovery will be tested monthly.

5. Develop a formalized IT replacement plan.

   A hardware replacement plan will be developed and incorporated into the IT Handbook

District officials should:

6. Implement a process for monitoring Internet use and enforcing the acceptable use policies.

   The District currently monitors Internet use using [redacted]. The District will establish a regular schedule to review and monitor Internet use not covered by [redacted] and enforce acceptable use policies.

7. Provide periodic IT security awareness training to all personnel who use IT resources, including the importance of appropriate use.

The IT Dept. will work with district administration to ensure all staff receive training in IT security awareness on [redacted].

8. Maintain accurate and up-to-date hardware and software inventories.

Our hardware inventory is maintained in database. We will review and make sure this inventory is current annually and codify this in IT Operations Manual. We will codify hardware replacement plan. We have installed [redacted] which will provide us with a software inventory on the Windows devices. IT will review reports from [redacted] annually. This too will be codified in the IT Operations Manual.

Non-instructional Employee Leave Benefits

Accrued Leave Was Not Adequately Recorded and Monitored

The Board did not develop a policy or written procedures for maintaining leave records. The District employs 166 non-instructional employees, in 15 different employee groups, who receive leave benefits (e.g., vacation, sick and personal leave) based on the terms negotiated in each of four employee CBAs or the annual Board-approved management confidential resolution. However, the processes used to request, approve and record leave were inconsistent from one employee group to the next, which allowed for different processes within a single negotiating unit. Throughout our audit, employees, department heads and officials expressed their lack of assurance that accrued leave balances were accurate.

The human resources clerk (clerk) is responsible for entering leave earned and used into the computerized leave tracking system. However, we found that she did not accurately enter these transactions in a timely manner. This process was further complicated because employees submitted leave requests electronically through another computerized software program, via email and on paper forms and the two systems were not interfaced. While the employees' direct supervisor approved their leave requests, supervisors were unable to verify whether the employee has sufficient available leave balances.

As of February 27, 2018, leave balances for 31 of the 40 non-instructional employees tested (78 percent) were inaccurate,[8] because the clerk did not properly process the leave requests. We reviewed 1602 properly approved leave request transactions, of which 122 were not recorded and 14 were inaccurately recorded in the leave tracking system.

Our review of recorded leave used disclosed that 14 entries lacked adequate support, such as an approved leave request. Entries made by the clerk to record leave earned each year for eight employees did not agree with the applicable CBA or Board resolution. Additionally, sick leave balances were understated by 39.63 days for eight employees and overstated by 52.26 days for 16 employees. Vacation leave balances were understated by 16.5 days for eight employees and overstated by 23.5 days for another eight employees. Further, personal leave balances were understated by .5 days for one employee and overstated by 6.5 days for six employees.

In addition to the immediate effect these inaccuracies have on employees, future employee leave payments upon leaving District employment could pose unnecessary costs for the District.

5 Two of the nine employees with accurate balances were new employees with no leave requests during our audit period. See Appendix B for information on our sampling methodology.

What Do We Recommend?

The Board should:

8

9. Develop a policy and written procedures standardizing a process for maintaining leave records and requests.

District officials should:

10. Ensure that leave earnings are granted per contract and Board approval and leave balance records are accurately maintained, correct and up-to-date.

11. Designate an independent individual to periodically review leave accrual records for accuracy.

12. Contact leave request vendor to set up the systems to directly interface.

The District developed uniform employee attendance procedures in each department and each school building. The Superintendent directed department heads and principals to follow these procedures.

DCSD Employee Attendance Procedures

1. ***All employees shall use the Aesop application to report absences and request approvals. Paper forms will be removed from offices in each school and department by supervisors and principals. Computer workstations are available for all employees. Aesop training shall be arranged by department supervisors.***

2. ***Building and department attendance clerks are responsible for ensuring that absences are properly recorded and reconciled in Aesop each day (not once/week). Attendance clerks shall report discrepancies to the principal or supervisor.***
   a. ***Attendance clerks are:***
      i. [redacted] - *EBH*
      ii. [redacted] - *DHS*
      iii. [redacted] - *DPS*
      iv. [redacted] - *Bus Garage*
      v. *TBA - Food Service*
      vi. [redacted] - *Special Programs*
      vii. [redacted] - *District Office and District Attendance Clerk (alternate* [redacted]*)*

3. ***The principal or supervisor shall investigate and address discrepancies.***

4. *Cleaners' attendance shall be reconciled by the attendance clerk in the building that each cleaner works in. A copy of cleaner schedule and time cards will be provided to each attendance clerk.*

5. *The GCC cleaners' attendance shall be reconciled at EBH. Names, schedules and time cards will be provided to attendance clerk.*

6. *Maintenance workers' attendance shall be reconciled at DPS.*

7. *The District Attendance Clerk will upload Aesop attendance into Envision each day. Payroll stubs shall accurately reflect employees attendance up to the time paychecks are run (typically the Wednesday before a Friday pay date or sooner if a pre-Friday pay).*

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 Board minutes and adopted IT and leave policies and procedures and interviewed District officials to gain an understanding of the District's IT and leave operations and determine the adequacy of the District's policies and procedures.
- We examined the account and security settings using specialized audit software. We reviewed the user and administrator accounts and compared them to current employee lists to identify inactive and unnecessary accounts. Further, we reviewed group policy automated settings and compared them to best practices.
- From various permissions reports and the account and security settings, we identified 334 users with permissions for various software containing PPSI, including the financial application, special education management software and student management systems. We assigned a value of "1" for each user and administrator. Based on the total risk score, of which the maximum was 5, we categorized the users into one of three risk levels (high, medium or low). We judgmentally selected a sample size for each risk category and randomly selected the users for our sample. In addition we judgmentally selected one computer that was marked for disposal to include in our testing.

Figure 1: Sample Composition

Risk Level	Total Number of Users	Percentage of Total Population	Computers in Our Sample	Percentage of Sample
High	7	2%	7	100%
Medium	147	44%	5	3%
Low	180	54%	2	1%
Computer Marked for Disposal			1	<1%
Total	**334**	**100%**	**15**	**4%**

We used specialized audit software to obtain web browsing histories, installed software and device settings for all 15 computers tested (we were unable to obtain a web history for one computer because it was out-of-date). We reviewed the device settings and analyzed the results to determine if they served a legitimate business purpose or presented any risk to the IT system.

- We compared identifiers for the sampled computers tested to the District's IT hardware inventory.

- During the performance of our testing we walked throughout the District's facilities and made observations of physical security controls.
- We reviewed the official electronic leave records, manual and electronic leave request records and leave accruals per contract or resolution to determine whether records of leave balances were maintained and whether leave used was posted accurately to the payroll records.

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 size of the relevant population and the sample selected for examination.

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 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. We encourage the Board to make the CAP available for public review in the District Clerk's office.

Appendix C: Resources and Services

Regional Office Directory
www.osc.state.ny.us/localgov/regional_directory.pdf

Cost-Saving Ideas – Resources, advice and assistance on cost-saving ideas
www.osc.state.ny.us/localgov/costsavings/index.htm

Fiscal Stress Monitoring – Resources for local government officials experiencing fiscal problems
www.osc.state.ny.us/localgov/fiscalmonitoring/index.htm

Local Government Management Guides – Series of publications that include technical information and suggested practices for local government management
www.osc.state.ny.us/localgov/pubs/listacctg.htm#lgmg

Planning and Budgeting Guides – Resources for developing multiyear financial, capital, strategic and other plans
www.osc.state.ny.us/localgov/planbudget/index.htm

Protecting Sensitive Data and Other Local Government Assets – A non-technical cybersecurity guide for local government leaders
www.osc.state.ny.us/localgov/lgli/pdf/cybersecurityguide.pdf

Required Reporting – Information and resources for reports and forms that are filed with the Office of the State Comptroller
www.osc.state.ny.us/localgov/finreporting/index.htm

Research Reports/Publications – Reports on major policy issues facing local governments and State policy-makers
www.osc.state.ny.us/localgov/researchpubs/index.htm

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

Contact

Office of the New York State Comptroller
Division of Local Government and School Accountability
110 State Street, 12th Floor, Albany, New York 12236

Tel: (518) 474-4037 • Fax: (518) 486-6479 • Email: localgov@osc.ny.gov

www.osc.state.ny.us/localgov/index.htm

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

ROCHESTER REGIONAL OFFICE – Edward V. Grant Jr., Chief Examiner

The Powers Building • 16 West Main Street – Suite 522 • Rochester, New York 14614-1608

Tel (585) 454-2460 • Fax (585) 454-3545 • Email: Muni-Rochester@osc.ny.gov

Serving: Cayuga, Chemung, Livingston, Monroe, Ontario, Schuyler, Seneca, Steuben, Wayne, Yates counties

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