Nicole Galloway, CPA
Missouri State Auditor

Waynesville R-VI School District

Student Data Governance

May 2016

Report No. 2016-025

http://auditor.mo.gov

Nicole Galloway, CPA
Missouri State Auditor

CITIZENS SUMMARY

Findings in the Cyber Aware Schools Audit of the Waynesville R-VI School District

Background	The Waynesville R-VI School District's Student Data Governance Audit was completed as part of the Cyber Aware School Audits Initiative. These audits are designed to assess the effectiveness of privacy and security controls with a focus on identifying practices to improve the security of information school districts have on students and their families. The district uses a student information system (SIS) to maintain student data and to track and monitor academic progress. The SIS maintains private and confidential data, such as social security numbers and assessment test scores. Additional systems and applications that maintain data are used for administrative functions and to enhance student productivity and classroom collaboration. The district relies extensively on computerized systems to support its educational and mission-related operations and on information security controls to protect the sensitive data residing on those systems. Auditors identified areas where improvements are needed but also found the district has developed certain controls to establish a safe environment for using technology, including promoting online safety, security, and confidentiality.
Data Governance	The district has not established a comprehensive data governance program, a critical task for any educational organization. A comprehensive program is necessary to ensure the confidentiality, integrity, availability, and quality of data. Without a formal program, the district cannot ensure that personally identifiable information (PII) is adequately protected and safe from unauthorized access, misuse, or inadvertent disclosure.
User Accounts	The district has not fully established controls for creating and maintaining user accounts for accessing system resources. Policies and procedures for disabling or removing user accounts timely after a user terminates are not documented. Auditors found 40 former users still had access to district systems 30 days or more after leaving the district. In addition, the district does not proactively monitor for user accounts that have not been accessed or used for a specified period of time. Certain staff share user accounts and passwords. However, these accounts are not monitored to ensure actions taken by users are appropriate. Without appropriate policies and procedures, including effective procedures to remove access and monitor for inactive accounts, users could continue to have access to critical or sensitive resources, which can provide opportunities for misuse or inappropriate disclosure of sensitive data.
Security Controls	The district has not implemented necessary security controls, leaving technology assets, including PII, at risk of inappropriate access, use, and disclosure. The district has not formally appointed any specific personnel to serve as security administrator or formally assigned responsibility for creating, implementing, and maintaining security policies and procedures. Without documented and approved policies and procedures, management lacks assurance that security controls are appropriate and properly applied.
Incident Response and Continuity Planning	The district has not taken all necessary measures to protect data in the event of a breach or other disruptive incident. The district has not formally documented policies and procedures for responding to security incidents,

has not adopted a formal data breach response policy, and has not completed the process of developing and testing a continuity plan. Without comprehensive incident response and breach-related policies, management may not be sufficiently equipped to respond quickly and effectively to an incident or breach, increasing the risk of potential harm to the district or affected individuals. Without a tested and functional continuity plan, management has limited assurance the organization's business functions and computer processing can be sustained during or promptly resumed after a disruptive incident.

Security Awareness Program	The district has not established a formal security and privacy awareness training program. As education organizations implement more powerful information systems and become more reliant on electronic data, proactive security awareness programs become increasingly important. With proper security and privacy awareness training and clear communication of data and device use policies, employees can become the first line of defense against cybersecurity incidents. However, without adequate training, users may not understand system security risks and their role in implementing related policies and controls to mitigate those risks.
Vendor Monitoring	The district has not established a process for ensuring software acquired or outsourced from information technology vendors complies with data security principles. Without an effective process for monitoring and managing risk of software acquisition or outsourcing, the district has less assurance in a vendor's ability to deliver services effectively, securely, and reliably and to ensure that services meet current and future data privacy and security needs.

Because of the nature of this report, no overall rating is provided.

All reports are available on our Web site: auditor.mo.gov

Waynesville R-VI School District Student Data Governance
Table of Contents

State Auditor's Report 2

Introduction
- Background 4
- Scope and Methodology 7

Management Advisory Report - State Auditor's Findings
1. Data Governance 9
2. User Accounts 10
3. Security Controls 12
4. Incident Response and Continuity Planning 16
5. Security Awareness Program 19
6. Vendor Monitoring 20

Organization and Statistical Information 21

NICOLE GALLOWAY, CPA
Missouri State Auditor

To the Board of Education
Waynesville R-VI School District

Due to increasing concerns for protecting the security and privacy of information schools maintain on students and the continued emergence of cyber threats, we have audited the Waynesville R-VI School District's student data governance program in fulfillment of our duties under Chapter 29, RSMo. This audit was conducted as part of the State Auditor's Cyber Aware School Audits Initiative and focused on evaluating the effectiveness of the data governance program, including identifying cybersecurity safeguards and privacy controls that can help schools improve the security of student data.

The objectives of our audit were to:

1. Evaluate the effectiveness of privacy plans and controls for safeguarding personally identifiable information.

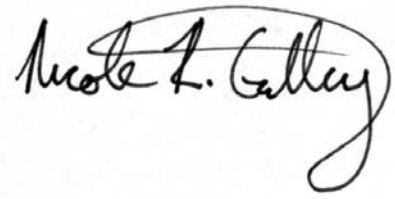
2. Evaluate the effectiveness of information security controls for protecting the confidentiality, integrity, and availability of significant systems and information technology resources.

3. Evaluate compliance with certain legal provisions.

We conducted our audit in accordance with the standards applicable to performance audits contained in *Government Auditing Standards*, issued by the Comptroller General of the United States. Those standards require that we plan and perform our audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides such a basis.

For the areas audited, we identified (1) the need to fully establish certain privacy plans and controls, (2) the need to fully establish certain information security controls for protecting the confidentiality, integrity, and availability of significant systems and information technology resources, and (3) no significant noncompliance with legal provisions.

The accompanying Management Advisory Report presents our findings arising from our audit of the Waynesville R-VI School District's student data governance program.



Nicole R. Galloway, CPA
State Auditor

The following auditors participated in the preparation of this report:

Deputy State Auditor:	Keriann Wright, MBA, CPA
Director of Audits:	Douglas J. Porting, CPA, CFE
Audit Manager:	Jeffrey Thelen, CPA, CISA
In-Charge Auditor:	Patrick M. Pullins, M.Acct., CISA
Audit Staff:	Marian Seevers, M.Acct., CPA
	Michelle Pummill

Waynesville R-VI School District Student Data Governance Introduction

Background

The Waynesville R-VI School District Student Data Governance Audit was completed as part of the Cyber Aware School Audits Initiative. These audits are designed to assess the effectiveness of privacy and security controls with a focus on identifying practices to improve the security of information school districts have on students and their families.

The district uses a student information system (SIS) to maintain student data and to track and monitor academic progress. The SIS maintains private and confidential data, such as social security numbers, assessment test scores, and other sensitive data. The district uploads various student data maintained in the SIS to the Department of Elementary and Secondary Education (DESE), Missouri Student Information System (MOSIS) Data Collection component periodically throughout the year. The MOSIS Data Collection component is used to collect student-level data from school districts for processing and reporting. Data submitted by the district includes elements such as enrollment and attendance, demographics, performance information, and college and career data used for evaluating the success and achievements of students. The district also uses a financial accounting system and a network management system for administering user access to various district resources. Other systems and applications are used for administrative functions and to enhance student productivity and classroom collaboration.

Cyber threats continue to emerge and evolve

As connectivity of business activity increases and organizations become increasingly dependent on technology, including computerized systems and electronic data, no school district is exempt from cyber threats, vulnerabilities, and privacy exposures. As a result, it is important to view information security and privacy as a business issue rather than strictly an information technology issue. Security threats, vulnerabilities, and privacy exposures challenge every organization, creating data protection and privacy risks that must be understood, addressed, and managed.

The National Institute of Standards and Technology (NIST) defines cybersecurity as the process of protecting information by preventing, detecting, and responding to attacks[1] while ISACA states cybersecurity encompasses all that protects enterprises and individuals from intentional attacks, breaches and incidents as well as the consequences.[2] Cybersecurity should be aligned with all other aspects of information security, including governance, management, and assurance. The state of being secure requires

[1] National Institute of Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity, Version 1, February 2014, is available at <http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf>.
[2] ISACA Cybersecurity Nexus, Transforming Cybersecurity, 2013, <http:// www.isaca.org/cyber>.

maintenance and continuous improvement to meet the needs of stakeholders and the demands of emerging cyber threats.

In the 2015 High-Risk Series[3] update, the Government Accountability Office (GAO) expanded the scope of the information security high-risk area to include protecting the privacy of personally identifiable information (PII).[4] The GAO expanded this risk area due to the challenges of ensuring the privacy of PII created by advances in technology. Technology advances, such as lower data storage costs and increasing interconnectivity, have allowed both government and private sector agencies to collect and process extensive amounts of PII more effectively. Risks to PII can originate from unintentional and intentional threats. These risks include insider threats from careless, disgruntled, or improperly trained employees and contractors; the ease of obtaining and using hacking tools; and the emergence of more destructive attacks and data thefts.

Technology advances, combined with the increasing sophistication of individuals or groups with malicious intent, have increased the risk of PII being compromised and exposed. Correspondingly, the number of reported security incidents involving PII in both the private and public sectors has increased dramatically in recent years. At the same time, school districts are increasingly reliant on technology and information sharing to interact with students and parents and to deliver essential educational services. As a result, the need to protect information, including PII, against cyber threats is increasingly important.

The Privacy Rights Clearinghouse[5] recorded breaches at kindergarten through grade 12 (K-12) educational institutions/school districts in the United States occurring during 2005 through 2015, potentially disclosing over 580,000 records of personal information.[6] These breaches include only

[3] Report GAO-15-290, Report to Congressional Committees, High-Risk Series An Update, February 2015, is available at <http://www.gao.gov/assets/670/668415.pdf>.

[4] According to the Family Educational Rights and Privacy Act (FERPA), personally identifiable information (PII) includes, but is not limited to (a) the student's name; (b) the name of the student's parent or other family members; (c) the address of the student or student's family; (d) a personal identifier, such as the student's social security number, student number, or biometric record; (e) other indirect identifiers, such as the student's date of birth, place of birth, and mother's maiden name; and (f) other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student.

[5] The Privacy Rights Clearinghouse is a nonprofit corporation whose mission is to engage, educate, and empower individuals to protect their privacy by raising awareness of how technology affects personal privacy.

[6] Privacy Rights Clearinghouse, Chronology of Data Breaches, is available at <http://www.privacyrights.org/data-breach>. We downloaded a file containing all breaches and filtered the results to include only data breaches occurring at K-12 educational institutions.

those made public and the data reflects three data breach incidents at Missouri public school districts.

Data governance

According to the U.S. Department of Education, Privacy Technical Assistance Center (PTAC),[7] data governance is an organizational approach to data and information management that is formalized as a set of policies and procedures encompassing the full life cycle of data, from acquisition to use to disposal. It includes establishing policies, procedures, and standards regarding data security and privacy protection, data inventories, content and records management, data quality control, data access, and data sharing and dissemination. Establishing a comprehensive data governance program helps ensure confidentiality, integrity, and availability of data and information by reducing data security risks due to unauthorized access or misuse of data.

Security and privacy controls

According to accepted standards, security controls are the management, operational, and technical safeguards or countermeasures prescribed for an information system to protect the confidentiality, integrity, and availability of a system and its information. Confidentiality refers to preserving authorized restrictions on information access and disclosure, including the means for protecting personal privacy and proprietary information. Integrity relates to guarding against improper information modification or destruction, and availability ensures timely and reliable access to and use of information. Effective privacy controls depend on the safeguards employed within the information system that is processing, storing, and transmitting PII and the environment in which the system operates. Organizations cannot have effective privacy without a basic foundation of information security. Without proper safeguards and controls, information systems and confidential data are vulnerable to individuals with malicious intentions who can use access to obtain sensitive data or disrupt operations.

Laws and regulations

Various federal and state laws and regulations pertain to the protection of sensitive student data, including the Family Educational Rights and Privacy Act (FERPA), the Individuals with Disabilities Education Act (IDEA), and the Protection of Pupil Rights Amendment (PPRA). Additionally, Section 161.096, RSMo, requires the State Board of Education to promulgate a rule regarding "student data accessibility, transparency, and accountability."[8]

[7] U.S. Department of Education, Privacy Technical Assistance Center, Data Governance Checklist, is available at <https://nces.ed.gov/programs/ptac/pdf/data-governance-checklist.pdf>.
[8] 5 CSR Section 20-700.100

Controls established

The district has an important responsibility for maintaining the privacy of student data and for implementing and maintaining information security controls. The district relies extensively on computerized systems to support its educational and mission-related operations and on information security controls to protect the sensitive data residing on those systems. While we found areas where improvements are needed, as discussed in the Management Advisory Report, we also found the district has established:

- A technology usage policy to facilitate access to district technology and to create a safe environment for using the technology, including promoting online safety, security, and confidentiality.
- Policies and procedures, including applicable parent/student forms, required to be in compliance with the FERPA data disclosure and usage provisions.
- The controls and processes required to be in compliance with the Children's Internet Protection Act (CIPA).
- Certain controls designed to help ensure the privacy of data and to help ensure the confidentiality, integrity, and availability of significant systems and data maintained on those systems.

Cyber threats will continue to challenge operational resilience and business continuity preparedness. School districts can reduce the risks of breaches by remaining aware of emerging cyber threats and consider the potential impact to operational resilience.

Scope and Methodology

The scope of our audit included the Waynesville R-VI School District's approach to data governance, including information security, privacy, and other relevant internal controls; policies and procedures; and other management functions and compliance issues in place.

Our methodology included reviewing written policies and procedures, and interviewing various district personnel. We obtained an understanding of the data governance approach and applicable controls that are significant within the context of the audit objectives and assessed whether such controls have been properly designed and placed in operation. We tested certain of those controls to obtain evidence regarding the effectiveness of their design and operation. We also obtained an understanding of legal provisions that are significant within the context of the audit objectives, and we assessed the risk that illegal acts, including fraud, and violation of contract or other legal provisions could occur. Based on that risk assessment, we designed and performed procedures to provide reasonable assurance of detecting instances of noncompliance significant to those provisions.

We obtained a list of district employees as of January 2016 from the district's accounting system. We matched these records to the user account records from the district's student information system, financial accounting

system, and network management system to determine if any terminated employees had active accounts. We also matched these records to users of the DESE statewide data collection systems. Although we used computer-processed data from these systems for our audit work, we did not rely on the results of any processes performed by these systems in arriving at our conclusions. Our conclusions were based on our review of the issues specific to the audit objectives.

We based our evaluation on accepted state, federal, and international standards; policies and procedures; and best practices related to information technology security and privacy controls from the following sources:

- National Institute of Standards and Technology (NIST)
- Government Accountability Office (GAO)
- ISACA (previously known as the Information Systems Audit and Control Association)
- U.S. Department of Education, Privacy Technical Assistance Center (PTAC)[9]

[9] According to its web site, the U.S. Department of Education established the PTAC as a "one-stop" resource for education stakeholders to learn about data privacy, confidentiality, and security practices related to student-level longitudinal data systems. The PTAC provides information and guidance on privacy, confidentiality, and security practices through a variety of resources. PTAC information is available at <http://nces.ed.gov/programs/ptac>.

1. Data Governance

The district has not established a comprehensive data governance program. As a result, there is less assurance the data management and protection procedures in place are effective in reducing data privacy and security risks due to unauthorized access or misuse of data.

According to the U.S. Department of Education, Privacy Technical Assistance Center (PTAC), data governance is necessary to ensure the confidentiality, integrity, availability, and quality of data. Establishing a data governance program is a critical task for any educational organization. An effective program requires establishing decision-making authority, defining policies and practices for the protection of sensitive data, identifying and gaining support of stakeholders, implementing the program, and monitoring its success. By clearly establishing policies, standard procedures, responsibilities, and controls for data activities, a data governance program helps to ensure that information is collected, maintained, used, and disseminated in a manner that protects privacy, confidentiality, and security, while allowing educational organizations to meet their missions.

During our review of the district's data governance approach, we found improvements are needed in the following component areas:

- Responsibility for data management
- Data stewardship
- Inventory and classification of data
- Source and content of data
- Monitoring unauthorized disclosure of personally identifiable information (PII)
- Archival and/or destruction of data at the end of its lifecycle

The district has not formally assigned responsibility for management of the district's data. Assigning appropriate levels of authority to data stewards and proactively defining the scope and limitations of that authority is a prerequisite to successful data management.

The district has not developed a formalized data stewardship plan documenting policies and procedures to protect student data. Adopting and enforcing clear policies and procedures in a written data stewardship plan is necessary to ensure that everyone in the organization understands the importance of data quality and security, and that staff are motivated and empowered to implement data governance.

The district does not maintain an inventory of data files, data elements maintained in those files, and the criticality or sensitivity of the data. Conducting an inventory of all data that require protection is a critical step for data security projects. Maintaining an up-to-date inventory of all

sensitive records and data systems, including those used to store and process data, enables the organization to target its data security and management efforts. Classifying data by level of sensitivity helps the data management team recognize where to focus security efforts.

The district has not formally identified the source and content of elements within the data files maintained by the district. Closely managing data content, including identifying the purposes for which data are collected, is necessary to justify the collection of sensitive data, optimize data management processes, and ensure compliance with federal, state, and local regulations.

The district has not implemented a monitoring process to detect unauthorized disclosures of PII within its custody. Ensuring the security of sensitive and personally identifiable data and mitigating the risks of unauthorized disclosure of these data is a top priority for an effective data governance program.

The district has not adopted a formal policy regarding the archival or destruction of data at the end of its lifecycle. While some data may need to be maintained indefinitely according to various laws and regulations, other data may become unnecessary or irrelevant when a student graduates or otherwise leaves the district, and can be destroyed when no longer needed. Planning for data archival or destruction is an integral part of a high quality data governance program, according to the U.S. Department of Education, PTAC. Data destruction is the process of removing information in a way that renders it unreadable (for paper records) or irretrievable (for digital records). Establishing policies and procedures governing the archival or destruction of data allows an organization to more efficiently and safely protect its data and is a critical component of an effective data governance program.

Without a formal data governance program, the district cannot ensure that PII maintained by the district is adequately protected and safe from unauthorized access, misuse, or inadvertent disclosure.

Recommendation

The district should establish and implement a formal data governance program encompassing the full life cycle of data, from acquisition to use to disposal.

Auditee's Response

The district concurs with the recommendation and will develop and implement a data governance program by July 2016.

2. User Accounts

The district has not fully established controls for creating and maintaining user accounts for accessing system resources. Accounts assigned to former employees or volunteers no longer working for the district are not always

removed timely, some accounts and passwords are shared by multiple users, and periodic monitoring to identify inactive accounts is not performed.

2.1 Terminated users

The district has not documented policies and procedures for disabling or removing user accounts timely after a user terminates. As of January 2016, 40 former users still had access to district systems and information 30 or more days after leaving the district, including one user who left in 2011.

While the district has procedures in place to notify information technology staff of a user's departure, the procedures are not documented and are not effective or consistently applied, as evidenced by the number of former users with active accounts. Additionally, the district does not periodically reconcile user accounts to district employees and volunteers.

Without effective procedures to remove access, terminated employees could continue to have access to critical or sensitive resources or have opportunities to sabotage or otherwise impair entity operations or assets, according to the Government Accountability Office (GAO).

2.2 Shared accounts

The district allows certain staff to share user accounts and passwords. However, these accounts are not monitored to ensure actions taken by users are appropriate.

The district maintains accounts for troubleshooting and testing various system settings and configurations, including security controls. Because the accounts are generically named and passwords are shared, any actions taken by the account users cannot be identified with a specific user. Additional compensating controls, such as monitoring or management review of actions performed using these accounts, are not in place.

Accepted standards require all users to have uniquely identifiable user accounts. Allowing multiple users to share the same account, without establishing compensating controls, makes it difficult, if not impossible, to identify the user responsible for changes made to system settings.

2.3 Inactive account monitoring

The district does not proactively monitor for user accounts that have not been accessed or used for a specified period of time.

Inactive accounts can indicate users no longer need the access privileges provided by the accounts and may be attractive targets for individuals attempting to gain unauthorized access since the account owners may not notice illicit activity on the accounts, according to the GAO. Without appropriate monitoring, security administrators are less likely to identify user accounts that had not been accessed or used for a specified period of time.

Recommendations

The district:

2.1 Fully establish, document, and follow policies and procedures to ensure user accounts and related access privileges are removed timely upon user termination.

2.2 Eliminate the use of shared accounts, or establish compensating monitoring controls to mitigate the risk of lack of individual accountability for system activity.

2.3 Periodically monitor user account access to identify and evaluate inactive accounts.

Auditee's Response

2.1 The district concurs with the recommendation and has created procedures and forms for user account removal of access privileges in a timely manner.

22 The district concurs with the recommendation and has eliminated the use of shared accounts for administrative testing.

2.3 The district concurs with the recommendation and has created a procedure and schedule for periodic inactive account reviews.

3. Security Controls

The district has not implemented all necessary security controls, leaving district technology assets, including PII, at risk of inappropriate access, use, and disclosure.

Logical security is the use of computer hardware and software to prevent or detect unauthorized access to systems, including the data therein. Logical security most often takes the form of user accounts and passwords, but also includes location and network based controls and security hardware, such as firewalls. Physical security is the protection of technology resources, including computers and network servers, from theft or damage. Physical security makes technology resources physically unavailable to unauthorized users and can include locked rooms and cabinets, periodic inventories of technology assets, and other measures to protect assets from unauthorized access.

3.1 Security administrator

The district has not formally appointed any specific personnel to serve as security administrator or formally assigned responsibility for creating, implementing, and maintaining security policies and procedures.

Accepted guidance from the U.S. Department of Education, PTAC states that organizations should develop comprehensive plans outlining organization policies and standards regarding data security and individual privacy protection. Such plans should clearly identify staff responsibilities

for maintaining data security and empower employees by providing tools they can use to minimize the risks of unauthorized access to PII.

Three district information technology staff have informally been tasked with maintaining security of the district's technology resources and data. However, without a formal designation of staff responsible for security administration, there is increased risk that security policies and procedures may not be adequately designed, documented, implemented, and updated.

3.2 Access controls

The district has not fully established policies and procedures regarding user access to systems and data. As a result, certain access controls needed to protect systems have not been implemented.

Logon banners

The district does not display logon banners to users accessing district systems and data.

Logon banners should display information to system users regarding applicable privacy and security notices and required compliance with applicable laws, regulations, and policies. According to accepted standards, logon banners should state that a user is accessing a district provided information system; that usage of the system may be monitored, recorded, and subject to audit; that unauthorized use of the system is prohibited and may be subject to criminal and civil penalties; and that use of the system constitutes agreement with the terms. Without a displayed logon banner, users may not be informed or aware of the authorized or appropriate use of the system and data.

Concurrent users

The district has not established controls to restrict concurrent access to district systems.

Concurrent session controls prevent a single user from accessing an information system from more than a specified number of locations at any given time. These controls help prevent unauthorized users from accessing the system by masquerading as an authorized user.

According to accepted standards, the number of concurrent sessions for a user should be limited. Without limiting access from multiple locations at the same time, management may not be able to ensure the confidentiality, integrity, and availability of data and the system.

3.3 Security logs

The district has not formally documented policies and procedures to identify the types of security events to be logged and monitored. As a result, there is less assurance that detected and logged security incidents are properly investigated and resolved.

The internal security policies within the district's network management system log thousands of entries each day. A majority of these entries, such as notification of successful login by system users, are of minimal use for security purposes. According to district staff, the network management system default logging settings are used. Because the district has not customized these settings regarding which events are logged, the security logs are voluminous and cannot effectively be monitored for unusual or suspicious activity.

Additionally, similar concerns exist for the network protection devices used by the district. One such system used by the district generated approximately 2.7 million recorded activities in a single 24-hour period. Only certain of these transactions are monitored via a report from the system. Most activities are not reviewed except upon special request, often to determine why certain activities were blocked and to request an exception be added to the system to allow future activity.

The district should establish relevant criteria and identify significant system events that should be logged. At a minimum, all such significant events, including access to and modification of sensitive or critical system resources, should be logged. Also, logging should include appropriate information to facilitate monitoring of such significant system events.

Without an effective method to identify, log, and monitor significant security-relevant events, the district is at increased risk that unauthorized or inappropriate system activity may not be detected.

3.4 Physical security

The district has not fully established physical security controls to ensure protection of technology resources. We noted the following risks:

- Responsibility for physical security of technology resources has not been formally assigned.
- A documented policy for physical access to technology resources, including who can be authorized access to restricted or sensitive areas, has not been established.
- Procedures for allowing temporary or guest access (contractors and vendors for example) to technology resources, such as escort and sign-in procedures, were not documented.

The effectiveness of physical security controls depends on the effectiveness of the organization's policies and practices pertaining to the overall facility and to areas housing sensitive information technology components. Without adequate physical security controls, the district is at risk the physical infrastructure of the computer network could be accidentally or maliciously damaged, destroyed, or lost; causing significant issues for the district.

3.5 Documentation of security controls

The district has not documented policies and procedures for certain security controls.

According to the GAO standards for internal control, control activities are an integral part of an organization's planning, implementing, reviewing, and accountability for stewardship of government resources and achieving effective results. Control activities are the policies, procedures, techniques, and mechanisms that enforce management's directives and helps ensure that actions are taken to reasonably address risks. The following control activities, including policies and procedures, have not been fully documented:

- Resetting lost or compromised passwords.
- Requesting and receiving approval for system access.
- Policies describing who may be granted privileged access to district systems.
- Notifying security administrators of the need to disable accounts for users terminating employment.
- Policies describing how to disable accounts for users terminating employment.
- Periodically reviewing user access to data and other information resources.

According to accepted standards, documentation of all aspects of computer support and operations is important to ensure continuity and consistency. Formalizing operational practices and procedures with sufficient detail helps to eliminate security lapses and oversights, gives new personnel sufficiently detailed instructions, and provides a quality assurance function to help ensure that operations will be performed correctly and efficiently.

Without documented and approved policies and procedures, management may not have assurance that control activities are appropriate and properly applied.

Recommendations

The district:

3.1 Formally appoint a security administrator who is responsible for developing and maintaining district security policies and procedures.

3.2 Fully establish access control policies and procedures by implementing logon banners for district systems to indicate appropriate use and by establishing security controls limiting the number of concurrent sessions for a single user.

3.3 Establish and document criteria for identifying which security events should be written to audit logs and monitored and investigated as security incidents.

3.4 Formally document responsibility for physical protection of technology resources and develop policies and procedures to effectively restrict physical access.

3.5 Fully document and periodically review security policies and procedures.

Auditee's Response

3.1 The district concurs with the recommendation and the administrator has been appointed by the Superintendent.

3.2 The district concurs with the recommendation and has implemented logon banners for district systems. The district is evaluating options for limiting concurrent sessions and will have a system in place by July 2016.

3.3 The district concurs with the recommendation and will create and implement a security auditing and response procedure by July 2016.

3.4 The district concurs with the recommendation and has assigned the responsibility to the Coordinator of Technology Services. Policies and procedures for physical access will be developed and implemented by July 2016.

3.5 The district concurs with the recommendations and will fully document security policies and procedures by July 2016. The policies and procedures will be reviewed annually.

4. Incident Response and Continuity Planning

The district has not taken all necessary measures to protect data in the event of a breach or other disruptive incident. The district does not have a complete incident response plan, has not adopted a formal data breach response policy, and has not fully documented and tested a continuity plan.

4.1 Incident response documentation

The district has not formally documented policies and procedures for responding to security incidents.

According to accepted standards, a security incident is an occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable

use policies. After an incident has been identified, appropriate action should be taken to identify and remedy the control weakness that allowed the violation to occur, repair any damage that has been done, and determine and discipline the perpetrator. It is important that an organization have formal written procedures for reporting security violations or suspected violations to a central security management office so that multiple related incidents can be identified, other employees alerted to potential threats, and appropriate investigations can be performed.

Without prompt and appropriate responses to security incidents, violations could continue to occur and cause damage to an organization's resources indefinitely. Further, violators will not be deterred from continuing inappropriate access activity, which could result in disclosure of confidential information and financial losses.

4.2 Data breach response policy

The district has not established a comprehensive data breach response policy. Implementing a data breach response policy is an essential step in protecting the privacy of student data.

A data breach is a security incident in which sensitive or confidential data, such as PII, has potentially been accessed, stolen, or used by an unauthorized individual. While the Family Educational Rights and Privacy Act (FERPA) does not contain specific breach notification requirements, the law requires recording of each data disclosure incident in the applicable record. However, the U.S. Department of Education, PTAC recommends all educational organizations create a data breach response policy, approved by the organization's leadership, that is germane to its environment. The policy should establish goals for the response process and include the definition of a breach, staff roles and responsibilities, as well as reporting, remediation, and feedback mechanisms. The policy should be well publicized and made easily available to all personnel whose duties involve data privacy and security protection.

Documenting and formalizing operational practices and procedures with sufficient detail helps to eliminate security lapses and oversights, gives new personnel sufficiently detailed instructions, and provides a quality assurance function to help ensure operations will be performed correctly and efficiently, according to accepted standards.

Without a comprehensive data breach response policy, management may not be sufficiently equipped to respond quickly and effectively in the event of a breach, increasing the risk of potential harm to affected individuals.

4.3 Continuity planning

The district has not documented and tested a complete continuity plan. Individuals responsible for carrying out those duties have not received formal training.

Elements of a continuity plan the district has not documented include:

- Priorities and procedures for the restoration of critical systems and data.
- Identification of persons responsible for restoration of specific systems and data.
- Formal identification of the resources and data included in the district's backups.

Additionally, while the district does backup data on a regular basis, a comprehensive test of backups to ensure that data can be successfully recovered in the event of a disaster has not been performed.

According to accepted standards, a continuity plan or suite of related plans should be developed for restoring critical business functions and applications. The plans should include arrangements for alternative processing facilities in case the usual facilities are significantly damaged or cannot be accessed. Staff should be trained and aware of their responsibilities to prevent, mitigate, and respond to emergency situations. For example, information security support staff should receive periodic training in emergency fire, water, and alarm incident procedures; and specific responsibilities for initiating and running an alternate data processing site.

Additionally, testing continuity plans is essential to determining whether the plans will function as intended in an emergency situation. The most useful scenarios involve simulating a disaster situation to test overall service continuity. Such an event would include testing whether the alternative data processing site will function as intended and whether critical computer data and programs recovered from off-site storage are accessible and current. Moreover, tests will assess how well employees have been trained to carry out their roles and responsibilities in a disaster situation. Any testing of continuity plans is likely to identify weaknesses in the plan, and it is important that the plan and related supporting activities, such as training, be revised to address these weaknesses. Otherwise, the benefits of the testing will be mostly lost.

District personnel provided auditors a draft of a newly developed continuity plan at the conclusion of audit fieldwork, indicating the district is making progress; however, the plan had not been formally approved, adopted, or tested. Without a tested and functional continuity plan, management has limited assurance the organization's business functions and computer processing can be sustained during or promptly resumed after a disruptive incident.

Recommendations

The district:

4.1 Establish and document an incident response plan that includes centrally tracking all security incidents.

4.2 Formally document and adopt a comprehensive data breach response policy to promote an appropriate response in the event of a breach of protected student data.

4.3 Complete the process of developing a comprehensive continuity plan and formally assign responsibilities for development, implementation, and maintenance of the plan to appropriate personnel. Once established, ensure the plan is tested on a periodic basis.

Auditee's Response

4.1 The district concurs with the recommendation and has created an incident response plan.

4.2 The district concurs with the recommendation and has created a data breach response procedure.

4.3 The district concurs with the recommendation and will develop a continuity plan by July 2016.

5. Security Awareness Program

The district has not established a formal security and privacy awareness training program. As education organizations implement more powerful information systems and become more reliant on electronic data, proactive security awareness programs become a priority. Uninformed users are a major threat to data security in education organizations.

According to accepted standards, the purpose of computer security awareness, training, and education is to (1) enhance security by improving awareness of the need to protect system resources and developing skills and knowledge so computer users can perform their jobs more securely; and (2) build in-depth knowledge, as needed, to design, implement, or operate security programs for organizations and systems. Additionally, guidance from the U.S. Department of Education, PTAC encourages organizations to provide security training on a recurring basis, communicate privacy policies to users, and define a process for reporting privacy incidents and complaints.

Making computer system users aware of their security responsibilities and teaching them correct practices helps users change their behavior. Awareness training also supports individual accountability, which is one of the most important ways to improve computer security. With proper security and privacy awareness training and clear communication of data and device

use policies, employees can become the first line of defense against cybersecurity incidents. However, without adequate training, users may not understand system security risks and their role in implementing related policies and controls to mitigate those risks.

Recommendation

The district establish a formal security and privacy awareness training program.

Auditee's Response

The district concurs with the recommendation. A security and privacy awareness training program will be mandatory for all staff prior to the beginning of the school year.

6. Vendor Monitoring

The district has not established a process for ensuring software acquired or outsourced from information technology vendors complies with data security principles.

The district utilizes software products from a number of vendors to manage financial information, human resources data, student data, and other information. Generally, the district pays an annual licensing/maintenance fee for these products. Depending on the arrangement, some products are installed on district-owned equipment and maintained by district personnel (with additional support from the vendor), while others are hosted and maintained directly by the vendor. In this case, district personnel access the system remotely, typically via a secure website.

We reviewed contracts for several systems or software products used by the district. Although the specific language varied, each contract had a clause stating the vendor would provide appropriate security functionality for the district. However, district staff indicated they had not asked any vendors to provide documentation that their product's security functionality met generally accepted industry standards.

Accepted standards require organizations to periodically review the overall performance of vendors, compliance to contract requirements, and value for money, and address identified issues. Without an effective process for monitoring and managing risk of software acquisition or outsourcing, the district has less assurance in a vendor's ability to deliver services effectively, securely, and reliably and to ensure that services meet current and future data privacy and security needs.

Recommendation

The district should develop procedures to formally monitor information technology vendors to ensure the district's data is properly protected and the vendor acts in accordance with contract terms and conditions.

Auditee's Response

The district concurs with the recommendation and will include in the district data governance plan.

Waynesville R-VI School District Student Data Governance Organization and Statistical Information

The Waynesville R-VI School District is located in Pulaski County.

The district operates a senior high school (grades 9-12), a middle school (grades 7-8), a sixth-grade center, five elementary schools (grades K-5 in various configurations), an early childhood center, and a career center. Enrollment was 5,795 for the 2015-2016 school year. The district employed 879 full- and part-time employees at December 31, 2015.

School Board and Key Personnel

An elected school board serves as the policy-making body for the district's operations. The board's seven members serve 3-year terms without compensation. Members of the board at December 31, 2015, were:

Dr. LeRoy Fulmer, President
Butch O'Riley, Vice President
Lisa Schwandt, Secretary
Dorsey Newcomb, Treasurer
Andy Anderson, Member
Mike Keeling, Member
Paul Shultz II, Member

Dr. Brian Henry serves as District Superintendent. Dr. Trish Adkins is the Assistant Superintendent for Instructional Services, and Mike Henson is the Director of Instructional Media and Technology Services.