



Office of Missouri State Auditor
Nicole Galloway, CPA

Park Hill School District

Student Data Governance



Nicole Galloway, CPA
Missouri State Auditor

CITIZENS SUMMARY

Findings in the Cyber Aware School Audit of the Park Hill School District

Background

The Park Hill 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 assessment test scores and other sensitive data. 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.

User Accounts

The district has not fully established controls for maintaining user accounts for accessing system resources. While certain procedures for removing access are in place, the district has not documented or fully established policies and procedures for disabling or removing user accounts timely after a user terminates. As of June 2016, three former district employees still had access to district systems and information 30 or more days after leaving the district. In addition, the district does not proactively monitor for student information system user accounts that have not been accessed or used for a specified period of time.

Security Controls

The district has not implemented all necessary security controls, leaving technology assets, including personally identifiable information, 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. Additionally, the district has not established adequate password controls to reduce the risk of unauthorized access to computers and data. Without documented and approved policies and procedures, management lacks assurance that security controls are appropriate and properly applied.

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

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

Park Hill School District Student Data Governance

Table of Contents

State Auditor's Report	2
------------------------	---

Introduction	
Background	4
Scope and Methodology	8

Management Advisory	
Report - State Auditor's	
Findings	
1. User Accounts	10
2. Security Controls	11

Organization and Statistical	15
Information	



NICOLE GALLOWAY, CPA

Missouri State Auditor

To the Board of Education
Park Hill 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 Park Hill 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 help schools improve the security of student data.

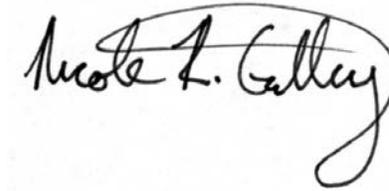
The objectives of our audit were to:

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 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 Park Hill School District's student data governance program.

A handwritten signature in black ink that reads "Nicole R. Galloway". The signature is written in a cursive style with a large, looping flourish at the end of the word "Galloway".

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:	Anh Nguyen

Park Hill School District Student Data Governance

Introduction

Background

The Park Hill 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 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 attacks¹ 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 maintenance and continuous improvement to meet the needs of stakeholders and the demands of emerging cyber threats.

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.



Park Hill School District Student Data Governance Introduction

In the 2015 High-Risk Series³ 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 Clearinghouse⁵ 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 those made public and the data reflects three data breach incidents at Missouri public school districts.

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.



Park Hill School District Student Data Governance Introduction

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

Data breach and response

In July 2014, the Park Hill school district publicly acknowledged a potential data breach of PII had occurred. A former district employee copied personal files to an external device to take upon leaving the district. However, some district-related documents, including files containing PII, were also copied.

⁷ U.S. Department of Education, Privacy Technical Assistance Center, Data Governance Checklist, is available at <http://ptac.ed.gov/sites/default/files/Data%20Governance%20Checklist%20%281%29.pdf>.

⁸ 5 CSR Section 20-700.100



Park Hill School District Student Data Governance Introduction

When the former employee connected the external device to a home network, certain files became publicly accessible on the Internet. A district patron discovered one of these files online and immediately notified the district.

The district took immediate action to secure the PII, with the full cooperation of the former employee, who had not realized the device contained PII. The district's investigation, which included the Federal Bureau of Investigation and an external contractor, determined only one file had been accessed one time (presumably by the patron who identified the issue and alerted the district). However the district opted to notify every individual who had PII on the device and arranged for one year of identity monitoring services at no cost. As of June 29, 2015, the district had not received any reports of PII being compromised or used in a fraudulent manner. As a result, the district did not extend coverage at the conclusion of the one year of monitoring services.

In addition to notifying the public, securing the PII, and offering identity monitoring services for individuals potentially affected; the district took measures to prevent similar incidents from occurring in the future, including updating policies related to employees' handling of sensitive information, enhanced training, and removing certain sensitive data from district systems.

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 data governance program designed to reduce data security risk.
- A data breach and incident response policy and plan to promote prompt response coordination.
- 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).
- Policies and procedures to help ensure services provided by information system vendors meet district needs and security and privacy requirements.



Park Hill School District Student Data Governance Introduction

- 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 Park Hill 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 June 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)



Park Hill School District Student Data Governance
Introduction

- 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>>.

Park Hill School District Student Data Governance Management Advisory Report State Auditor's Findings

1. User Accounts

The district has not fully established controls for maintaining user accounts for accessing system resources. Accounts assigned to former employees no longer working for the district are not always removed timely and periodic monitoring to identify inactive accounts is not performed.

1.1 Terminated users

While certain procedures for removing access are in place, the district has not documented or fully established policies and procedures for disabling or removing user accounts timely after a user terminates. As of June 2016, three former district employees still had access to district systems and information 30 or more days after leaving the district.

Access to most district computer systems is controlled through an interface between the district's Human Resources (HR) computer system and the district's network management system. User accounts in the network management system are automatically created or disabled when a user is added or removed from the HR system. However, the three former employees identified had access to systems not controlled by this process, meaning their access had to be manually added or removed.

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).

1.2 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:

- 1.1 Fully establish, document, and follow policies and procedures to ensure user accounts and related access privileges are removed timely upon user termination.
- 1.2 Periodically monitor user account access to identify and evaluate inactive accounts.

Auditee's Response

- 1.1 *The district will continue to improve the implementation of existing documented policies and procedures to ensure user accounts and*



Park Hill School District Student Data Governance
Management Advisory Report - State Auditor's Findings

related access privileges are removed in a timely manner upon termination.

1.2 *The district will continue to improve documented policies and procedures to monitor user accounts and related access.*

2. Security Controls

The district has not implemented all necessary security controls, leaving district technology assets, including personally identifiable information (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.

2.1 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.

The district technology director has 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.

2.2 Password controls

The district has not established adequate password controls to reduce the risk of unauthorized access to computers and data. Passwords are required to authenticate network access, however, controls to enforce the use of strong passwords have not been required.

The network management system provides the functionality for administrators to enforce strong password controls such as specifying the maximum length of time a password may be used before it has to be



Park Hill School District Student Data Governance
Management Advisory Report - State Auditor's Findings

changed, preventing the reuse of a certain number of previously used passwords, and specifying password length and complexity requirements (such as a mix of upper and lower case characters, numbers, and special characters). However, the password policy implemented by the district does not use all of the available functionality to enforce the use of strong passwords. In addition, while authorized users must first logon to the network management system, separate passwords for accessing an administrative system are not required to be changed periodically.

Not enforcing strong password controls increases the risk of a password becoming known by someone other than the account owner, which may result in inappropriate access to and misuse of sensitive district information.

2.3 Security logs

The district has formally documented policies and procedures to identify the types of security events to be logged and monitored. However, the policies need to be enhanced to provide assurance that all significant security incidents are detected, logged, and 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. While certain security events are logged, according to district policy, failed attempts to access district resources are not logged.

The district should enhance criteria for identifying significant system events that should be logged. At a minimum, all such significant events, including unauthorized access to sensitive or critical system resources, should be logged. Without identifying, logging, and monitoring significant security-relevant events, the district is at increased risk that unauthorized or inappropriate system activity may not be detected.

2.4 Concurrent users

The district has not established controls to limit or detect 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 or detecting 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.

2.5 Documentation of security controls

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



Park Hill School District Student Data Governance
Management Advisory Report - State Auditor's Findings

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 at the time of our audit:

- The allowable use of removable media, such as flash drives.
- Resetting lost or compromised passwords.
- Policies describing who may be granted privileged access to district systems.
- Periodic reviews of user groups, including membership and the access rights granted to the groups.

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:

- 2.1 Formally appoint a security administrator who is responsible for developing and maintaining district security policies and procedures.
- 2.2 Enhance password controls to prevent unauthorized access to computers and data.
- 2.3 Enhance existing criteria for identifying which security events should be written to audit logs and monitored and investigated as security incidents.
- 2.4 Manage and monitor the number of concurrent sessions for a single user.
- 2.5 Fully document and periodically review security policies and procedures.



Park Hill School District Student Data Governance
Management Advisory Report - State Auditor's Findings

Auditee's Response

- 2.1 *The district has formally appointed the director of technology as the security administrator who is responsible for developing and maintaining district security policy and procedures.*
- 2.2 *The district has enhanced existing password controls to prevent unauthorized access to computers and data.*
- 2.3 *The district will continue to use existing processes to regularly review established criteria for identifying which security events are written to audit logs, monitored and investigated as security incidents.*
- 2.4 *The district will review the recommendation to manage and monitor the number of concurrent sessions for a single user.*
- 2.5 *The district will continue to use existing processes to fully document and periodically review established security policies and procedures.*

Park Hill School District Student Data Governance Organization and Statistical Information

The Park Hill School District is located in Platte County.

The district operates two high schools (grades 9-12), three middle schools (one grade 6, two grades 7-8), ten elementary schools (grades K-5), an early education center (pre-K), an alternative education center, and an aquatic center. Pre-K through grade 12 enrollment was 11,533 for the 2015-2016 school year. The district employed 2,403 full- and part-time employees at April 30, 2016.

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 April 30, 2016, were:

Matt Pepper, President
Janice Bolin, Vice-President
Bart Klein, Treasurer
Susan Newburger, Member
Todd Fane, Member
Karen Holland, Member
Boon Lee, Member

Dr. Jeanette Cowherd serves as District Superintendent. Dr. Paul Kelly is Assistant Superintendent for Business and Technology, and Derrick Unruh is the Director of Technology.