Third Party Relationships

Internal Audit Report

November 17, 2020

Orange County Public Schools
Internal Audit

Linda J. Lindsey, CPA, CGAP, School Board Internal Auditor
Alpa H. Vyas, CIA, CRMA, Senior Internal Auditor

Table of Contents

EXECUTIVE SUMMARY

Why We Did This Audit

Our objectives were to determine whether management has addressed findings from our previous (2017) audit and, evaluate the district's current management of risks associated with third party relationships.

This audit was included in the 2019-2020 Annual Audit Plan.

Observations and Conclusion

Audit Results at a Glance			
	Risk/Impact Rating		
Results and Observations	Significant	Moderate	Minor
IA – Internal or M - Management	IA - 4	IA - 2	-
D - Deficiency or O - Opportunity	D - 4	D - 1 O - 1	-

We commend management for progress made since our previous audit. Most notably:

- Improved contract provisions related to data security are included in more contracts.
- ITS has adopted a *Third Party Information Security Standard* effective 3/12/2020 (*Standard*).

However, we urge further improvement of third party risk management through full adoption and enforcement of the third-party vendor management processes established in the *Standard*.

Results and Recommendations

Breaches of data are a continuing concern in the education industry and educational institutions are attractive targets because they are data-rich. To help OCPS manage these risks, we made the following recommendations, the first two of which are repeated from our previous audit.

Repeat:

- The district should have a comprehensive inventory of all third party relationships and a structured vendor management process.
- Software acquisitions should follow the established process and be purchased only after all approvals are given and not from school internal funds.

New:

- Develop and implement employee training on risks associated with sharing data with third parties, OCPS' various data security policies, and safeguarding of data as called for in the *Standard*.
- Carefully evaluate risks of piggyback contracts with vendors who have access to PII information.
- As required by the *Standard*, during the contracting phase, request and evaluate vendors' internal controls over secured data, subcontractors, disaster recovery/ business continuity plan, and cyber insurance information.
- User management should know about third parties' subcontractors and their internal controls over secured data.
- User management should obtain compliance reports from vendors, review reports periodically to identify risks not addressed by vendors, and take steps to mitigate those risks.
- All contracts should have clauses for Protection and Handling of Data, FERPA, and Force Majeure.

This report has been discussed with management and they have prepared their response, which follows.

DEFINITIONS:

Risk / Impact Ratings

Minor	Low risk with a financial impact of less than one percent and/or an isolated occurrence limited to local processes (low impact and low likelihood)
Moderate	Slight to moderate risk with a financial impact between one and five percent and/or a noticeable issue that may extend beyond local processes (low impact and high likelihood or high impact and low likelihood)
Significant	High risk with a financial impact greater than five percent and/or a significant issue that occurs in multiple processes (high impact and high likelihood)

Observations Categories

Deficiency	A shortcoming in controls or processes that reduces the likelihood of achieving goals related to operations, reporting and compliance
Opportunity	A process that falls short of best practices or does not result in optimal productivity or use of resources

Criteria for Observations Sourced to Management

- Internal audit was informed of the issue prior to starting detailed testing
- Management identified, evaluated, and communicated the issue to appropriate levels of the district
- Management has begun corrective action with clear, actionable plans and targeted completion dates

None of the observations resulting from this audit were sourced to management.

BACKGROUND:

Third Party Risk

Like many organizations, OCPS relies on outside providers of products and services to achieve its strategic objectives, deliver a high quality education, and operate efficiently and effectively. When we provide services ourselves, our internal control processes work to reduce risk to acceptable levels. When we decide to have those services provided by third parties, risks are beyond the reach of our internal control processes and we depend on the internal controls of the third parties.

A third party's risk is the district's risk. Holding vendors to high standards of physical and cyber security, internal controls, personnel management, and regulatory compliance can be challenging, but it is essential. Third party risk management is a process of assessing and controlling the reputational, financial, and legal risks posed by parties outside the district. A strong third party risk management program will help reduce our risks.

OCPS Examples

The district has many relationships with third parties that require access to district data in order to provide services to the district. These relationships are critical to the district's operations, but they bring increased risks. Examples include:

Table 1

Examples of Critical Relationships with Vendor		
Contract/Department	**Services**	**Types of Data Accessed**
Career Staff Unlimited, LLC. (Piggyback) / ESE Instructional Support	Speech and Language Therapy	IEPs, students' health records through Skyward
CSI Nurse World, Inc. / ESE Health and Behavior Services	Nursing	ESE students health records through Skyward
AMIKids Orlando, Inc. / Alternative Education Service - BETA	Juvenile Justice Program	"At-Risk" students' data through Skyward
iCiMS / HR Talent Management	Applicant Tracking System	Applicants' personal information

When we decide to have services provided by third parties, risks are beyond the reach of our internal control processes.

A third party's risk is the district's risk.

Third party risk management involves assessing and controlling:

- *Reputational,*
- *Financial, and*
- *Legal risks.*

Relationships with third parties are critical to district operations but they also bring risks.

Examples of third party relationships involving access to district data.

Industrial Physical Capability Services / Risk Management & ESE	Pre-Employment Strength Screening	Job candidates' health data

Previous Audit

We last audited third party risks in late 2017 and issued our report titled, *Data Management of Third Party/Vendor Relationships*, on January 23, 2018. The overall conclusion of this previous audit was that district management should improve its oversight processes in assessing and controlling risks associated with third parties that collect, manage, process, or store district data.

Our previous audit of third party risks concluded that the district needed to improve oversight processes.

ITS Standard

The ITS Information Security Office recently established a standard titled, *Third Party Information Security Standard* (*Standard)*, effective March 12, 2020, which addresses the risks associated with third-party relationships. (See *Appendix A*.)

A recent ITS Standard addresses third party relationships.

OBJECTIVES, SCOPE AND METHODOLOGY:

Objectives

Our objectives were to:

- Determine whether management has addressed findings from the previous audit; and,
- Evaluate the district's current management of risks associated with third party relationships by:
    - Determining whether contracts with third parties having access to district data contain provisions that address confidentiality, protection, reporting of breaches, and other important data protection matters;
    - Determining whether district personnel are evaluating vendors' controls over data during the selection process and are monitoring vendor performance related to data protection compliance during the contract term;

Our first objective was to determine whether management had addressed findings from the previous audit.

- Determining whether any breaches have occurred and how they have been handled; and,

Scope

The scope of the audit included contracts in place between July 1, 2018 and March 31, 2020. This scope included contracts executed before and after new terms and conditions that address protection and handling of data were adopted in July 2018.

Our scope included contracts in place between July 1, 2018 and March 31, 2020.

Methodology

Out audit methodology included:

- Reviewing School Board policies such as EHB – *Data and Records Retention, Computer Database Resources,* and EHBA – *Records Management (Public Records)*;
- Reviewing Management Directives A-9 *Employee Use of Technology*, A-15 *Employee Responsibility In The Proper Use Of Sensitive Data,* and B-2 *Use Of Social Media;*
- Determining whether management has implemented the actions indicated in their response to our previous audit;
- Inquiring of the Senior Director of Information Security for selected Information Technology Services (ITS) contracts and overall data security;
- Reviewing ITS standards and guidelines such as *Third Party Information Security Standard, Enforcing the SSN Policy, Guidelines for Acceptable Use of Network Resources*, *OCPS Data Loss Prevention FAQ,* and *OCPS Proofpoint Secure Email FAQ;*
- Reviewing a judgmentally selected sample of 22 contracts and related documents;
- Determining whether any training on data security/protection guidelines was held;
- Verifying with user departments' management:
  - whether vendors are handling and securing OCPS data;
  - whether any supply chain vendors are involved with the third party;

We reviewed School Board policies, Management Directives, prior audits, ITS guidelines and Standard.

We selected 22 contracts for evaluation.

  - whether users' management is maintaining/reviewing Service Organization Control (SOC) reports, testing/audit reports, or other control documents over data, and cyber liability coverage insurance, if any; and,
  - whether there has been any impact of the COVID-19 pandemic on vendors' activities.
- Reviewing selected vendors' corporate websites for their policies addressing data security, data protection, data processing, business continuity, disaster recovery, and SOC reports;
- Reviewing Purchase Orders (POs) and invoices in SAP and confirming whether any payments were made during the COVID-19 pandemic if selected vendors were not providing any services/products;
- Reviewing the district software approval process and testing 15 randomly selected software purchases from School Funds Online (SFO) and four from the Teaching and Learning (T&L) approved software list; and,
- Reviewing district POs and invoices from SAP and school POs and invoices from school bookkeepers, confirming whether software was approved prior to purchase, and reviewing Non-Disclosure Agreements (NDAs), if required.

We evaluated user departments' management of third party contracts.

We tested 19 software purchases to confirm whether the approval process was followed.

Our audit was conducted in accordance with the *International Standards for the Professional Practice of Internal Auditing* of the Institute of Internal Auditors and included such procedures as deemed necessary to provide reasonable assurance regarding the audit objective. Internal Auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.

Our audit was conducted in accordance with the International Standards for the Professional Practice of Internal Auditing.

We are required to note any material deficiencies in accordance with Florida Statutes, School Board Policy and sound business practices. No material deficiencies were noted in this audit. We also offer suggestions to improve controls or operational efficiency and effectiveness.

There were no material deficiencies.

RESULTS AND RECOMMENDATIONS:

Overall Conclusion:

We commend management for progress made since our previous audit. Most notably:

- Improved contract provisions related to data security are included in more contracts.
- ITS has adopted a *Third Party Information Security Standard* effective 3/12/2020 (*Standard*).

Management has made progress since our last audit.

ITS Information Security has adopted a Third Party Information Security Standard (see Appendix A).

However, we urge further improvement of third party risk management through full adoption and enforcement of the third-party vendor management processes established in the *Standard*. The complete *Standard* is located in *Appendix A* to this report. Our detailed findings and recommendations follow.

Repeat Comments:

1) *The district should have a comprehensive inventory of third party vendor relationships and a structured vendor management process.* *Significant Risk*

The district should have an inventory of all third party relationships.

Best Practice:

Evaluate where we have exposure in the collection, use, and management of different types of data by maintaining an accurate and complete inventory of all third party relationships and their associated risks. The vendor inventory would identify third parties that

- have access to and/or store sensitive date,
- provide infrastructure or core business services,
- are key to our business continuity plan, and
- need to be reviewed because of regulations

Identify vendors, risks and criticality to our operations to determine whether our total risk exposure falls within tolerance levels.

and rank them by risk and priority to our operations. This makes it easier to identify the critical vendors and the critical functions each performs on our behalf so that we can see our total risk exposure and determine whether it falls within our risk tolerance.

The inventory is a key part of an overall vendor management process that includes:

- evaluation of risks and performance of due diligence before contracts are engaged,
- strong contract language,
- monitoring after contract services begin, and
- periodic re-evaluation of risks during the contract term.

Vendor management involves procedures before and after contract execution and during the contract term.

Audit Results:

The comprehensive inventory of existing third party relationships involving data has not been prepared, nor has the district fully implemented a due diligence processes to evaluate risks associated with these relationships before we sign contracts or processes to monitor vendor performance related to these risks after contract execution. Monitoring vendor performance after contract execution is particularly in need of attention.

Monitoring vendor performance after contract execution is particularly in need of attention.

The ITS Information Security Department is charged with establishing and enforcing enterprise policies and standards related to information and network security and availability. Accordingly, ITS Information Security developed *Third Party Information Security Standard* (*Standard*), effective 3/12/2020, which establishes security requirements for third parties that handle OCPS' confidential information. The *Standard* sets forth detailed actions that should occur during the pre-acquisition, acquisition, and operations phases of third-party vendor relationships.

The ITS Third Party Information Security Standard includes detailed procedures for an inventory and due diligence procedures.

Recommendation:

1) The district should develop a comprehensive inventory of all third party relationships involving data sharing as stated in *Third Party Information Security Standard*, and implement and enforce the due diligence actions included in the *Standard*.

The district should implement and enforce the ITS Standard.

2) ***Schools purchased software from internal accounts; purchased without the approvals of ITS and/ or T&L; and, purchased after approval was denied.*** ***Significant Risk***

Schools purchased software from internal accounts and purchased without required approvals. One school purchased software after approval was denied.

Best Practice:

Schools should comply with district policies and procedures and not circumvent approval processes.

Audit Results:

Our previous audit found that schools purchased software without approval. They accomplished this in several ways, including purchasing before the approval process was complete, circumventing the approval process, purchasing without required non-disclosure agreements (NDAs), and purchasing despite a denial. Management's response was to communicate to school principals regarding policy and procedures for purchasing instructional software.

This finding is a repeat of what we noted in our previous audit.

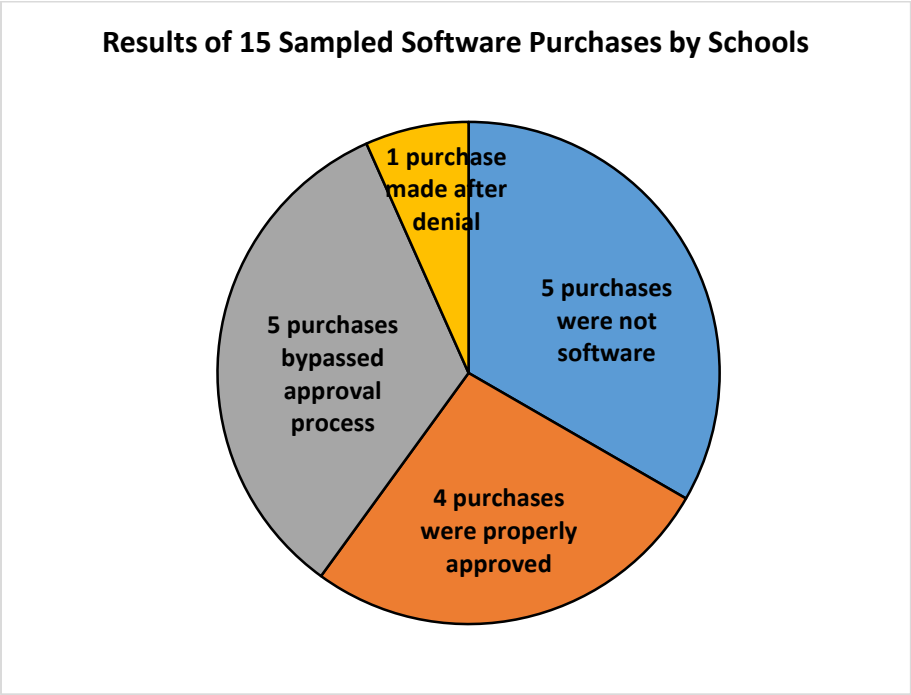
This audit revealed that schools are continuing to purchase software without ITS and/ or T&L approvals by circumventing the approval process. As noted in the previous audit, they do this by acquiring software from school funds which bypasses the ITS approval process.

The district's Instructional Software Approval process evaluates whether an NDA is required.

We judgmentally selected 15 transactions in School Funds Online (SFO) that appeared to be for software. The schools' principals approved each of the 15 selected transactions. Five of the selected purchases were not for software. The other 10 of these transactions were for software, and of those, four had followed the established approval process (except for using internal funds) while five did not and one purchase occurred after approved had been denied. The following chart shows the results of our sample.

A signed NDA helps to ensure that the vendor protects the confidentiality of shared information.

Chart 1



We evaluated ten software purchases by schools and noted six that did not follow the established approval process.

The following table shows detailed information for the seven software purchases with exceptions. These vendor relationships may call for NDAs.

Table 2

Information for Software Acquired Bypassing Approval		
Bypassed Approval Process		
Vendor	**Function**	**School**
Varsity News Network Inc.	Graphic Software Annual Fee	Jones HS
Software 4 Schools	Election / Voting	Boone HS
Music Sales Corp.	Music Software	Blanker K-8
Computer Medicine Sports Inc.	EMR Software	Winter Park HS
Track Wrestling Com LLC.	Online Tournament Mgmt. Software	East River HS and Windermere HS
Purchased After Approval was Denied		
J&W Pepper and Son Inc.	Music Software	Dr. Phillips HS

There is a risk to student data if schools bypass the approval and evaluation process for NDA.

Recommendations:

- Software acquisitions should follow the established process and be purchased only after all approvals are given. Employees who fail to follow the processes should be subject to discipline.
- Prohibit purchases of software from internal funds to ensure integrity of the approval process.

Current Comments:

3) *Employees who manage third party contracts need training on data protection/data security of district data within those third party relationships.* ***Moderate Risk***

Employees who manage third party contracts need training on data protection/ data security.

Best Practice:

The best strategy to protect data shared with third parties is to train employees on awareness of data protection/data security, risks of sharing data with those third parties, and mitigation of those risks by setting/evaluating adequate controls.

ITS Third Party Information Security Standard includes such a requirement for *awareness training for OCPS personnel that interact with third parties regarding appropriate rules of engagement based on the type of third-party and level of access to OCPS information assets.*

The ITS Standard on third party information security includes a requirement for training employees on third party relationships involving district data.

Audit Results:

Breaches are a major concern in the education industry since technology is an integral part of educational record systems and educational institutions are attractive targets because they are data-rich.

Breaches are a major concern in the education industry. Educational institutions are attractive targets because they are data-rich.

We noted that employees who manage third party contracts receive no training on:

- awareness of data protection/data security,
- management of district data, or
- evaluation of risks associated with third parties who handle/manage different types of data.

Recommendation:
ITS Information Security should develop and implement employee training on risks associated with sharing data with third parties, OCPS' various data security policies, and safeguarding of data as called for in the *Standard*.

A piggyback contract with a vendor having access to students' PII did not contain the district's data protection and handling provisions.

4) A piggyback contract with a vendor having access to students' PII information does not contain the district's data protection and handling provisions. *Moderate Risk*

Best Practice:
When piggybacking other entities' contracts, the district's data protection and handling provisions should supplement the piggyback agreement to ensure protection of district's data if the vendor has access to PII information.

Audit Results:
Three piggyback contracts were in our sample of 22 contracts and one of those gives the vendor access to students' PII information through Skyward. The piggyback contract mentioned Health Insurance Portability and Accountability Act (HIPAA) requirements but did not include the district's Protection and Handling Data provision.

The district should carefully evaluate risks of piggyback contracts with third parties having access to data.

Recommendation:
The district should carefully evaluate risks of piggyback contracts with vendors who have access to PII information and supplement the original contract with the district's contract language.

5) Adherence to ITS' Third-Party Information Security Standard procedures during the sourcing and purchasing process should address risks associated with vendors' subcontractors, control adequacy and effectiveness, disaster recovery and business continuity, and cyber liability insurance. *Significant Risk*

ITS' Third-Party Information Security Standard describes factors that must be evaluated during the sourcing and contracting phase.

Requirements of the Standard:

The *Standard* states that certain factors must be evaluated during the sourcing and contracting phase of procurement. Among those factors are:

- the use of other third parties (subcontractors)
- the adequacy of the third-party's policies and procedures relating to internal controls in accordance with Report on Controls of Service Organizations such as SOC1/SOC2
- business resumption contingency planning
- the adequacy of the third-party's insurance coverage

Audit Results:

Subcontractors - User departments could not provide compliance evidence reports, e.g. SOC or other. Additionally, most of the selected contracts' user management are not aware of their vendors' subcontractors (supply chain vendors) such as fourth and fifth parties and associated risks.

User departments did not know about subcontractors of vendors that handle our data.

SOC Reports - There is no formal process to request vendors' compliance evidence during the sourcing and contracting phase, or to maintain, review, or monitor vendors' compliance reports. We found that some of the selected vendors do issue SOC reports and will provide them upon request and have privacy/confidentiality policies and/ or data security/ processing policies. However, contract users were unaware and not accessing or evaluating this information.

The district is not obtaining SOC reports.

Business Continuity - Out of 22 sampled contracts, 14 did not include language of vendor's business continuity, staff retention, and/or disaster recovery plan. From the remaining eight contracts, three vendors have established business continuity and disaster recovery plans based on their Recovery Time Objectives and Recovery Point Objectives, and these are available upon request. Others have some business continuity/ disaster recovery or staff availability language.

Vendors' business continuity is not addressed in a number of contracts.

Cyber Liability Insurance - Some contracts referenced professional liability insurance, technology errors and omissions (E&O) insurance, and cyber insurance. Professional liability insurance protects vendors during a data breach. E&O insurance and cyber insurance help vendors

The district is not evaluating vendors' cyber liability insurance.

manage client risk and cover vendors' liability for a data breach involving their customer's information. The district does not have a practice to review and evaluate vendors' cyber liability insurance during the sourcing and contracting phase. We noted that some vendors provide cyber insurance certificates upon request.

Comply with the Standard.

Recommendation:
Comply with the *Standard*.

6) *The district's standard contract provisions addressing Protection and Handling (P&H) of Data, Family Educational Rights and Privacy Act (FERPA), and Force Majeure were missing in selected sample contracts.* ***Significant Risk***

Best Practice:
The district's Procurement and Legal Departments have adopted standard terms and conditions that are expected to be used in all district contracts. Among these terms and conditions are provisions that deal with Protection and Handling of Data, Family Educational Rights & Privacy Act (FERPA), and Force Majeure.

The district has very good contract terms addressing protection and handling of data, student data and Force Majeure.

The Protection and Handling of Data (P&H Data) provision addresses the vendor's requirement to safeguard district data, comply with related federal and state laws and report data breaches. FERPA is a federal law that addresses privacy of student data. Force Majeure is a contractual defense that excuses parties from contractual obligations during specific situations and frees both parties from liability.

Audit Results:
Out of 22 sampled contracts, eight have the P&H Data provision while others have some language addressing confidentiality, privacy, protection of data, and HIPAA. One contract has no language regarding data protection and confidentiality.

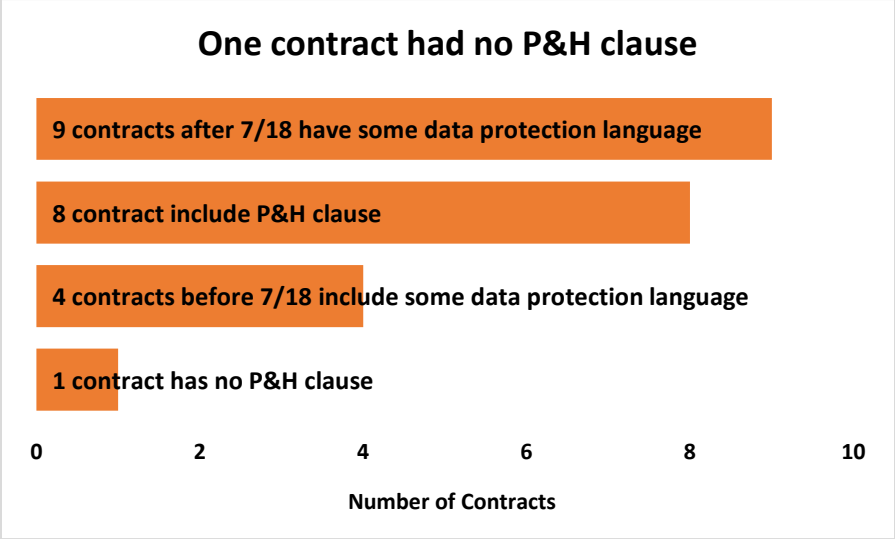
We noted a number of contracts that did not include the district's standard terms and conditions related to data.

Out of 22 sampled contracts, six do not have the FERPA provision. Per Director of Procurement, FERPA is applicable to every purchase made and all POs include a FERPA clause.

All except five of the selected sample contracts have Force Majeure provisions. Per Director of Procurement, Force Majeure is applicable to every purchase made and all POs include a Force Majeure clause.

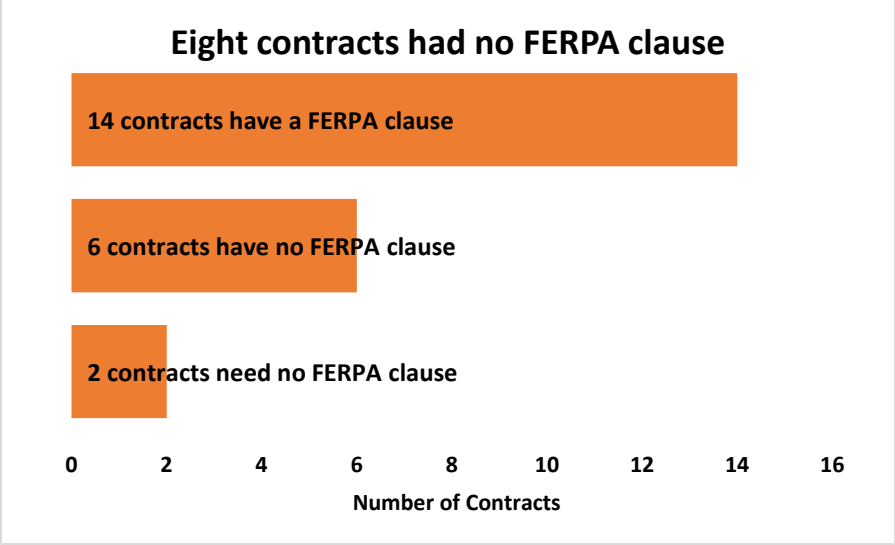
The following charts provide details of the sample results.

Chart 2



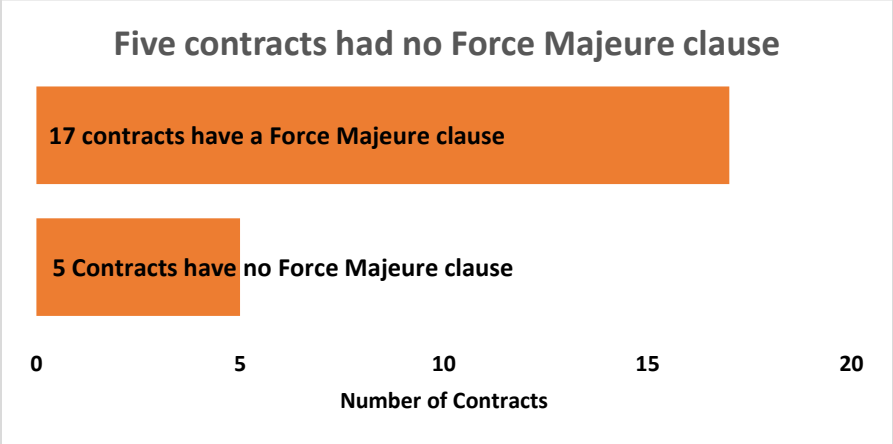
Sample results for Protection and Handling of Data.

Chart 3



Sample results for FERPA.

Chart 4



Sample results for Force Majeure.

Recommendation:

Include standard terms and conditions dealing with Protection and Handling of Data, FERPA and Force Majeure in all contracts.

We wish to thank those from many departments who cooperated and assisted in this audit.

ORANGE COUNTY PUBLIC SCHOOLS

THIRD-PARTY INFORMATION SECURITY STANDARD

Document ID#: ITS_InfoSec_006

Contents

DOCUMENT CHANGE CONTROL

DOCUMENT NAME:	**OCPS Third-Party Information Security Standard**
DOCUMENT ID:	**ITS_InfoSec_006**
EFFECTIVE DATE:	
LAST REVISED DATE:	**1/9/2020**

Version No.	Revised by	Effective Date	Description of Changes
0.90	Mike Sanchez	04/01/2019	Publication Development
1.0	Russell Holmes	1/9/2020	Review and Update
	Russell Holmes	3/12/2020	Review and Update
			Pre-publication review
			Approved for Publication by:

DOCUMENT OWNER

The owner of this document is the OCPS Chief Information Security Officer (CISO) (or designee). It is the responsibility of the document owner to maintain, update and communicate the content of this document. Questions or suggestions for improvement should be submitted to the document owner.

ANNUAL REVIEW

This **Third-Party Information Security Standard** should be reviewed and updated by the document owner on an annual basis or when significant policy or procedure changes necessitate an amendment.

RELATED DOCUMENTS

Document	Effective date
ITS_InfoSec_007 - Enterprise Data Loss Prevention	3/12/2020

1 PURPOSE

1.1 This standard establishes security requirements for the use of third parties that handle OCPS confidential information, either by storing, processing, transmitting or receiving information. This standard outlines the following controls to reduce the information security risks associated with contracted services and staff:

- Identification of risks related to ***third parties*** to ensure appropriate protection of OCPS ***information assets***
- Definition of information security requirements for ***third-party*** agreements
- ***Third-party*** information management oversight from contract initiation through termination

2 AUTHORITY

2.1 The ITS Information Security Department has been charged with the establishment and enforcement of enterprise policies and standards as they are related to information and network security and availability. These policies and standards include, but are not limited to, network and internet access and any device connecting to the OCPS wired or wireless network as well as cloud or local applications/systems that collect personally identifiable information (PII), protected health information (PHI), financial, or other data that OCPS wishes to protect.

3 SCOPE

3.1 This document applies to the use of information, information systems, electronic and computing devices, applications, and network resources used to conduct business on behalf of OCPS. The document applies to all OCPS offices including all executive offices, boards, schools, departments, divisions, councils, bureaus, and offices within an executive office. Other OCPS entities that voluntarily use or participate in services provided by the District must agree to comply with this document, with respect to those services, as a condition of use. All OCPS offices are required to implement procedures that ensure their ***personnel*** comply with the requirements herein to safeguard information.

4 RESPONSIBILITY

4.1 The ITS Information Security Department is responsible for the development and ongoing maintenance of this ***standard***. The ITS Information Security Department is responsible for this ***standard*** and may enlist other departments to assist in the monitoring and maintenance of compliance with this ***standard***.

4.2 Any inquiries or comments regarding this ***standard*** shall be submitted to the ITS Information Security Department at ITSInformationSecurity@OCPS.net.

5 COMPLIANCE

5.1 Compliance with this document is mandatory for the District and its affiliates including all executive offices, boards, schools, departments, divisions, councils, and bureaus. Violations are subject to disciplinary action in accordance to applicable employment and collective bargaining agreements, up to and including the termination of their employment and/or assignment with OCPS.

5.2 Exceptions to any part of this document must be requested via email to the ITS Information Security Office. A policy exception may be granted only if the benefits of the exception outweigh the increased risks, as determined by OCPS' CISO.

6 STANDARD STATEMENTS

6.1 Third-Party Selection

As part of the ***third-party*** selection process, OCPS Offices and Agencies must ensure that the items listed below are evaluated from a security perspective during the sourcing and contracting phases:

6.1.1 Technical and industry experience

6.1.1.1 Identify areas where OCPS may have to supplement the ***Third-Party***'s capabilities related to information management to fully manage risk to OCPS' ***information assets***.

6.1.1.2 Evaluate the ***Third-Party***'s use of other ***third parties***' (i.e., subcontracting relationships) technology to support the contracted operations.

6.1.1.3 Evaluate the experience of the ***Third-Party*** in providing services that include the handling of ***confidential*** information in the anticipated operating environment.

6.1.1.4 Evaluate the ***Third-Party***'s ability to respond to service disruptions (see *Incident Management and Business Continuity and Disaster Recovery* standards).

6.1.2 Operations and control (as applicable)

6.1.2.1 Determine/review the adequacy of the **Third-Party's** policies and procedures relating to internal controls in accordance with Report on Controls of Service Organizations such as SOC1/SOC2 User/Client Control Considerations (e.g., parameters, logical access, event logs/audit trails), facilities management, privacy protections, maintenance of records, business resumption contingency planning, secure systems development and maintenance and state employee background checks.

6.1.2.2 Determine whether the **Third-Party** provides enough security precautions, including, when appropriate, firewalls, encryption and customer identity authentication, to protect OCPS information resources as well as detect and respond to intrusions.

6.1.2.3 Evaluate whether OCPS has complete and timely access to the information maintained by the **Third-Party** both during and after any Third-Party engagement.

6.1.2.4 Evaluate the **Third-Party's** knowledge of regulations (e.g., FERPA, COPAA, PCI) that are relevant to the services they are providing.

6.1.2.5 Assess the adequacy of the **Third-Party's** insurance coverage in consultation with risk management or procurement functions.

6.2 Contractual Security Risk Identification

All contracts by which a **Third-Party** provides services to OCPS or allows a **Third-Party** to access, store, process, analyze or transmit OCPS **confidential information** shall be assessed, prior to entering into an agreement, to determine the **Third-Party**'s

capability to maintain the confidentiality, integrity and availability of OCPS **information assets** consistent with the Enterprise Information Protection Requirements Standard. The following shall be considered during **third-party** sourcing and/or contract negotiation:

6.2.1 ***Third-party*** sourcing and contract negotiation

6.2.1.1 Organizational objectives and requirements.

6.2.1.2 Transparency to evaluate and manage **third-party** relationships.

6.2.1.3 Importance and criticality of the services to OCPS (see Asset Management and Communication and Network Security Standard).

6.2.1.4 Defined requirements for the contracting activity, including any potential regulatory requirements.

6.2.1.5 Necessary security controls/reporting processes required by OCPS Executive Offices and Agencies.

6.2.1.6 Contractual obligations and requirements to be imposed on the Third-Party.

6.2.1.7 Contingency plans, including the availability of alternate third parties, costs and resources required to switch third parties upon breach or termination (see IS.TBD Business Continuity and Disaster Recovery standards)

6.3 Contractual Security Provisions

OCPS Offices and Agencies must ensure that Information Security policies and requirements are addressed and documented in any contract with the ***Third-Party***. Provisions shall be established in the contract to protect the security of OCPS' ***information assets***.

6.3.1 ***Third-party*** contracts must address the following, where applicable:

6.3.1.1 All parties involved with the agreement must be made aware of their privacy and security responsibilities and are required to sign confidentiality agreements (e.g., non-disclosure agreement).

6.3.1.2 Information classification requirements in accordance with OCPS' Information Classification and Information Protection Requirements standards.

6.3.1.3 Relevant legal and regulatory requirements which may apply to information processed, stored or transmitted.

6.3.1.4 Requirements governing the acceptable use of OCPS-owned or managed information.

6.3.1.5 The means by which a ***Third-Party*** proposes to transfer information to other ***third parties*** and will require written notice and agreement from OCPS prior to any such transfer.

6.3.1.6 Adherence by the ***Third-Party*** to an information security program, including, but not limited to, password and access management requirements, physical security of facilities and servers containing OCPS information, network protection, system and software protection, encryption and information security of data in transit and at rest, and intrusion-detection/prevention systems.

6.3.1.7 Training and awareness requirements for specific procedures and information security requirements (e.g., for incident response, authorization procedures).

6.3.1.8 Screening requirements, if any, for ***third-party*** personnel, including responsibilities for conducting the screening and notification procedures if screening has not been completed or if the results give cause for concern.

6.3.1.9 OCPS explicitly reserves the right to audit the performance of information security and other contractual responsibilities of the parties involved in the signed agreement. This will be done when deemed necessary by an OCPS organization and doing so will incur no additional cost to a OCPS' contract.

6.3.1.10 Third-Party's obligation to periodically deliver an independent report on the effectiveness of controls (e.g., SOC1/SOC2, vulnerability testing results) and agreement on timely correction of relevant issues raised in the report.

6.3.1.11 Processes used by the Third-Party to report incidents in writing to OCPS involving any type of security breach or unauthorized access to OCPS' information assets within the appropriate timeframes (see Incident Management Standard).

6.3.1.12 Upon termination of the contract, OCPS information will be transmitted to OCPS or OCPS' ***Third-Party*** of choice in a format defined by OCPS at a cost specified to the mutual satisfaction of OCPS and the Third-Party prior to termination.

6.3.1.13 Processes used to electronically erase, render unreadable or physically destroy all OCPS' information assets upon termination of the agreement (see Information Disposal Standard).

6.3.1.14 OCPS explicitly reserves the right to request, at any time, transfer or purging of some or all information stored on third-party systems at a cost specified to the mutual satisfaction of OCPS and the Third-Party prior to termination.

6.3.1.15 Maintenance and testing procedures for Business Continuity Planning as appropriate.

6.3.1.16 Enabling processes to provide for timely forensic investigation in the event of a compromise.

All contracts shall be reviewed by Legal for accurate content, language and presentation. If the information being collected or exchanged is ***confidential***, a binding non-disclosure agreement shall be in place between OCPS and the ***Third-Party***, whether as part of the contract or a separate non-disclosure agreement (required before any confidential information is shared).

6.4 Third-Party Life Cycle Management

OCPS Offices and Agencies must ensure that all third parties shall be managed through the life cycle of the contract by the Information Owner in collaboration with the Information Security Team and Procurement/Legal.

6.4.1 The following shall be considered throughout the ***third-party*** life cycle management process:

6.4.1.1 Inventory of third parties with assigned vendor risk rating.

6.4.1.2 Contractual performance criteria or service-level agreements.

6.4.1.3 Contractual, regulatory or legal requirements.

6.4.1.4 Inventory of all relevant contractual deliverables.

6.4.1.5 Information classification of information entrusted to third parties.

6.4.1.6 Enablement of accounts used by third parties for remote access only during the time period needed and monitor remote access accounts when in use.

6.4.1.7 Audit provisions to determine the Third-Party's compliance per defined requirements.

6.4.1.8 The frequency of audit based on advice from functions such as Internal Audit, Information Security and Legal.

6.4.1.9 Communicate the need for transition or return of information at end of engagement/contract and obtain certification in writing from the Third-Party that all OCPS information has been permanently deleted if the contract so requires.

6.4.1.10 Risk assessment at the onset and at least annually thereafter and upon significant changes to the agreement or environment. The risk assessment shall identify critical assets, threats and vulnerabilities and result in a formal, documented analysis of risk. Significant changes include:

6.4.1.10.1 Changes and enhancement to networks.

6.4.1.10.2 Use of new technologies.

6.4.1.10.3 Adoption of new products or newer versions or releases.

6.4.1.10.4 New development tools and environments.

6.4.1.10.5 Changes to the physical location of service facilities.

6.4.1.10.6 Subcontracting to another Third-Party.

6.4.1.11 Awareness training for OCPS personnel that interact with **third parties** regarding appropriate rules of engagement based on the type of **Third-Party** and level of access to OCPS **information assets**.

7 APPENDIX – CONTROL MAPPING

SELECTION	SP 800-53 R4	CIS 20	CSF
6.1 Third-party Selection	CA-2	CSC 4	ID.RA-1
	CA-3	CSC 1	ID.AM-3
	SA-9	-	ID.AM-4
	AC-1	-	ID.GV-1
	AU-1	-	ID.GV-1
	CA-1	-	ID.GV-1
	CM-1	-	ID.GV-1
6.2 Contractual Security Risk Identification	CP-1	-	ID.GV-1
	IR-1	-	ID.GV-1
	MA-1	-	ID.GV-1
	PE-1	-	ID.GV-1
	PL-1	-	ID.GV-1
	PM-1	-	ID.GV-1
6.3 Contractual Security Provisions	PS-1	-	ID.GV-1
	AT-1	-	ID.GV-1
	RA-1	-	ID.GV-1
	RA-2	-	ID.AM-5
	SA-1	-	ID.GV-1
	SA-6	-	-
6.4. Third-party Life Cycle	RA-3	CSC 4	ID.RA-1
	AT-1	-	ID.GV-1
	RA-1	-	ID.GV-1
	RA-2	-	ID.AM-5
		-	ID.AM-6
		-	ID.BE-1

Appendix B – SOC Reports

When an organization engages a vendor to perform key functions, the organization exposes itself to additional risks related to the vendor's system. Although management can delegate functions to a vendor, responsibility for the service cannot be delegated. Vendor management is essential when vendors perform functions that are critical to district operations and/ or when they involve our data. Experience has shown that questionnaires, assurances, and contractual clauses alone are not sufficient for these vendors. In these cases, vendors that serve multiple organizations should provide special types of audit reports, called Service Organization Controls (SOC) reports.

<table>
<tr><th colspan="4">SOC 1 vs SOC 2</th></tr>
<tr><td colspan="2">Focus: Financial Transaction & Security Processing Controls</td><td colspan="2">Focus: Security Controls</td></tr>
<tr><td colspan="2">Objective: Validate controls over completeness and accuracy of monetary transactions and financial statement reporting.</td><td colspan="2">Objective: Certify the security, processing integrity, availability, confidentiality and/or privacy of hosted systems and the data they store or process.</td></tr>
<tr><td colspan="2">Control objectives: Defined by vendors</td><td colspan="2">Control objectives: Standardized</td></tr>
<tr><td colspan="2">OCPS examples: school internal accounting system, payment card processing, Medicaid billing services, etc.</td><td colspan="2">OCPS examples: data center, student information system, applicant tracking system, third party claims administration, etc.</td></tr>
<tr><td>Type 1</td><td>Type 2</td><td>Type 1</td><td>Type 2</td></tr>
<tr><td>Vendor systems & controls
• At a specific time point
• Key security issues
• Audit opinion on design of controls</td><td>Vendor systems & controls
• Over a period of time
• Audit opinion on design & operating effectiveness of controls</td><td>Vendor system & controls
• At a specific time point
• Focus on security
• Audit opinion on design of security controls</td><td>Vendor system & controls
• Over a period of time
• Audit opinion on design & operating effectiveness of security controls</td></tr>
</table>

There is also a SOC 3 report that covers the same testing procedures as a SOC 2 report, but does not provide a system description or detailed test results. These are for general use, often in marketing materials, and are not suitable for an organization's vendor management program.

Some vendors should provide both SOC 1 and SOC 2 reports because their customers will require assurances about both financial and security controls. Examples include financial services, healthcare, or insurance, and others that deal with sensitive user data.

Department / School Name	**Third Party Relationships**
Administrator / Department Head	
Cabinet Official / Area Superintendent	**Chiefs**

Audit Result / Recommendation	Management Response Acknowledgement/ Agreement of Condition	Responsible Person (Name & Title) And Target Completion Date	Management's Action Plan
1) ***The district should have a comprehensive inventory of third party vendor relationships and a structured vendor management process.*** ***Recommendations:*** The district should develop a comprehensive inventory of all third party relationships involving data sharing as stated in *Third Party Information Security Standard,* and implement and enforce the due diligence actions included in the *Standard.*	ITS and Procurement currently have a comprehensive inventory of software for all software that is placed through the procurement process and/or through the software approval process. In the case of non-ITS related agreements, end-users manage the compliance of all terms of the agreement including Third Party Information Security Compliance.	Robert Curran, Chief Information Officer Russell Holmes, Sr. Director, Information Security 11/2020 All District Divisions Chiefs. 06/2021	ITS will continue to encourage anyone that purchases software to follow the software approval process. The district will remind all end users of their roles and responsibilities when managing a contract. Managers will assess third-party relationships to determine level of risk and appropriate mitigating strategies. An analysis will be conducted to determine the feasibility of centrally inventorying all information based on available resources.

2) ***Schools purchased software from internal accounts; purchased without the approvals of ITS and/ or T&L; and, purchased after approval was denied.*** **<u>Recommendations:</u>** Software acquisitions should follow the established process and be purchased only after all approvals are given. Employees who fail to follow the processes should be subject to discipline. Prohibit purchases of software from internal funds to ensure integrity of the approval process.	We currently have a process in place. Purchasing software directly from internal accounts is already prohibited in district internal account procedures.	Maria Vazquez, Deputy Superintendent 12/2020 Dale Kelly, Chief Financial Officer Shari Horsey, Director of Finance 12/2020	Process for purchasing software is in place. Employees violating the process will be reminded of process. Repeated offenses could result in disciplinary action. The Internal Accounts Handbook will be revised to specifically state the prohibition against purchasing software from internal account funds as opposed to the broader prohibition against purchasing computer related equipment directly from internal accounts.
3) ***Employees who manage third party contracts need training on data protection/data security of district data within those third party relationships.*** **<u>Recommendation:</u>** ITS Information Security should develop and implement employee training on risks associated with sharing data with third parties, OCPS' various data security policies, and	ITS Information Security will work with Procurement in creating training/guidelines as it relates to the risks associated with sharing data with third parties, OCPS' various data security policies, and safeguarding of data. Create a training document that will	Robert Curran, Chief Information Officer Russell Holmes, Sr. Director, Information Security 04/2021	ITS will create a training document that will be shared with all administrators who will share with their employees.

safeguarding of data as called for in the *Standard*.	shared with all administrators to be shared with their employees.		
4*) A piggyback contract with a vendor having access to students' PII information does not contain the district's data protection and handling provisions.* **Recommendation:** The district should carefully evaluate risks of piggyback contracts with vendors who have access to PII information and supplement the original contract with the district's contract language.	In addition to the standard contract review process, the applicable language may be included in piggyback agreements to further address data protection and handling provisions.	Roberto Pacheco, Chief Operations Officer Robert Waremburg, Senior Director of Procurement Services 03/2021	Procurement Services will continue to evaluate the risks of piggyback contracts with vendors who have access to PII information and supplement the original contract with the district's contract language with assistance from the end-user departments.
5) *Adherence to ITS' Third-Party Information Security Standard procedures during the sourcing and purchasing process should address risks associated with vendors' subcontractors, control adequacy and effectiveness, disaster recovery and business continuity, and cyber liability insurance.* **Recommendation:** Comply with the *Standard*.	Procurement Services will continue to assure compliance with the standard.	Roberto Pacheco, Chief Operations Officer Robert Waremburg, Senior Director of Procurement Services 03/2021	Procurement Services will formalize the process that includes ITS as part of the review process and department end users for non-ITS related contracts to ensure the contracts address the Third-Party Information Security Standard procedures and risks associated with vendors' subcontractors, control adequacy and effectiveness, disaster recovery and business continuity, and cyber liability insurance.

6) ***The district's standard contract provisions addressing Protection and Handling (P&H) of Data, Family Educational Rights and Privacy Act (FERPA), and Force Majeure were missing in selected sample contracts.*** **Recommendation:** Include standard terms and conditions dealing with Protection and Handling of Data, FERPA and Force Majeure in all contracts.	District Purchase Orders contain terms and conditions addressing data protection and handling data, FERPA, and Force Majeure. Additional terms and conditions that mirror those included on all formal solicitations will be added to address any possible gaps.	Roberto Pacheco, Chief Operations Officer Robert Waremburg, Senior Director of Procurement Services 03/2021	Procurement Services will expand the inclusion of standard terms and conditions dealing with Protection and Handling of Data, FERPA, and Force Majeure in all purchase orders and contracts.