TECHNOLOGY SERVICES

1050 Main Street • Roseville, CA 95678
Phone (916) 771-1645 • Fax (916) 771-1650
Laura Assem, Director of Technology

Vendor Statement of Compliance for Data Privacy and Protection

This agreement is entered into between **Roseville City School District** ("LEA") and ScholarChip Card LLC ("Service Provider") 05/03/19 ("Effective Date".)

WHEREAS, the LEA and the Service Provider entered into an agreement for Educational Technology services;

WHEREAS, the LEA is a California public entity subject to all state and federal laws governing education, including but not limited to California Assembly Bill 1584 ("AB 1584"), the California Education Code, the Children's Online Privacy and Protection Act ("COPPA"), and the Family Educational Rights and Privacy Act ("FERPA");

WHEREAS, AB 1584 requires, in part, that any agreement entered into, renewed or amended after January 1, 2015 between a local education agency and a third-party service provider must include certain terms;

NOW, THEREFORE, the Parties agree as follows:

Section I: General (All data)

1. **PASSWORD SECURITY.** All passwords are considered secure. Vendors may not disseminate any passwords unless specifically directed by Educational or Technology Services management. Vendors will not provide information concerning Admin accounts (ROOT Admin, container Admin, local NT administrator or Domain administrator) or their equivalent to any persons. District personnel ONLY will disseminate this information. Vendors will never create "back door" or "generic" user accounts on any systems unless specifically directed to do so by LEA management.
   Agree: Yes X No _____

2. **SYSTEM SECURITY.** Unauthorized access to or modification of District systems including file servers, routers, switches, NDS and Internet services is prohibited. Any attempt to bypass or subvert any District security system, both hardware and software is prohibited.
   Agree: Yes X No _____

3. **PRIVACY.** The vendor will adhere to all provisions of the Federal Family Educational Rights and Privacy Act (FERPA, 20 U.S.C. 123g), California Education Code and District policies regarding the protection and confidentiality of data. At all times, the vendor will consider all data collected in the course of their duties to be protected and confidential. Release of this data can only be authorized by Technology & Information Services management and state and federal law.
   Agree: Yes X No _____

TECHNOLOGY SERVICES

1050 Main Street • Roseville, CA 95678
Phone (916) 771-1645 • Fax (916) 771-1650
Laura Assem, Director of Technology

4. **REUSE**: Vendors shall not copy, duplicate, sell, repackage or use for demonstration purposes any Roseville City School District data without the prior, written consent of Educational and Technology Services management.
   Agree: Yes X No _____

5. **TRANSPORT**: Vendor must provide a secure channel (S/FTP, HTTPS, SSH, VPN, etc) for the District to "push" data to the vendor and to extract data as required. Vendors will not have direct access to District systems and will not "pull" data at any time.
   Agree: Yes X No _____

6. **EXTERNAL SECURITY:** Vendor must attach to this document reasonable evidence that their system is secure from external hacking and attacks. Devices such as firewalls and technologies such as NAT are the minimum requirements. Active IDS or similar technology is preferred.
   Agree: Yes X No _____

7. **INTERNAL SECURITY:** Vendors must attach to this document reasonable evidence that their system is secure from internal hacking and attacks. Describe the interactions vendor personal (or their representatives) will have directly with District data. How is uploaded data from the District handled and processed? Who has access to this data? What happens to the data after the upload is complete? What security safeguards are in place to protected unauthorized access to District data? How are backup performed and who has access to and custody of the backup media? How long are backup maintained; what happens to the District data once the backup is "expired"? If any data is printed, what happens to these hard copy records?
   Agree: Yes X No _____

8. **DISTRICT ACCESS:** Vendor must provide a secure means (see Item 5 above) for the District to extract ALL data from the vendor system. This can either be an online extraction tool or a vendor provided extract as needed by the District (not to exceed quarterly). Describe the means and format of the data (delimited, Excel, MDB, SQL Dump).
   Agree: Yes X No _____

9. **TERMINATION:** Upon termination of this agreement as provided herein, vendor will permanently delete all customer data from their system as allowed by state and federal law. Vendor may be required to certify destruction of LEA data within 90 days of contract termination.
   Agree: Yes X No _____

10. **NOTICE OF BREACH:** Vendor must notify Roseville City School District's Superintendent and Director of Technology of any breach to the security of the system or breach in the security of the data, in the most expedient time possible and without unreasonable delay (Cal. Civ. Code §1798.29).
    Agree: Yes X No _____

TECHNOLOGY SERVICES

1050 Main Street • Roseville, CA 95678
Phone (916) 771-1645 • Fax (916) 771-1650
Laura Assem, Director of Technology

Section II: AB1584 Compliance (Student information only)

1. Vendor agrees that the Roseville City School District retains ownership and control of all student data.
   Agree: Yes X No _____

2. Vendor must attach to this document a description of how student created content can be exported and/or transferred to a personal account
   Agree: Yes _____ No N/A

3. Vendor is prohibited from allowing third-parties access to student information beyond those purposes defined in the contract
   Agree: Yes X No _____

4. Vendor must attach to this document a description of how parents, legal guardians and students can review and correct their personally identifiable information
   Agree: Yes X No _____

5. Vendor will attach to this document evidence how student data is kept secure and confidential
   Agree: Yes X No _____

6. Vendor will attach to this document a description of procedures for notifying affected parents, legal guardians or eligible students when there is an unauthorized disclosure of student records
   Agree: Yes X No _____

7. Vendor certifies that student records will not be retained or available to a third party once the contract has expired or is canceled (See Page 2, Item 9).
   Agree: Yes X No _____

8. Vendor will attach to this document a description of how they and any third party affiliates comply with FERPA
   Agree: Yes X No _____

9. Vendor and its agents or third parties are prohibited from using personally identifiable information from student records to target advertising to students
   Agree: Yes X No _____

TECHNOLOGY SERVICES

1050 Main Street • Roseville, CA 95678
Phone (916) 771-1645 • Fax (916) 771-1650
Laura Assem, Director of Technology

Section III: SB 1177 SOPIPA Compliance (Student information only)

1. Vendors cannot target advertising on their website or any other website using information acquired from students
   Agree: Yes X No _____
2. Vendors cannot create a profile for a student except for school purposes as defined in the executed contract
   Agree: Yes X No _____
3. Vendors cannot sell student information
   Agree: Yes X No _____
4. Vendors cannot disclose student information unless for legal, regulatory, judicial, safety or operational improvement reasons
   Agree: Yes X No _____
5. Vendors must attach to this document evidence of how student information is protected through reasonable security procedures and practices
   Agree: Yes X No _____
6. Vendors must delete district-controlled student information when requested by the school district
   Agree: Yes X No _____
7. Vendors must disclose student information when required by law, for legitimate research purposes and for school purposes to educational agencies.
   Agree: Yes X No _____

As an authorized representative of my organization, I accept the conditions listed in this document.

Laura Assem — 7/8/2019

Roseville City School District — Date

Donna J. Harrigan — 5/3/19

Donna Harrigan, Director of GRC, ScholarChip — Date

TECHNOLOGY SERVICES

1050 Main Street • Roseville, CA 95678
Phone (916) 771-1645 • Fax (916) 771-1650
Laura Assem, Director of Technology

Exhibits

Section I.6 External Security:

See ScholarChip Data Security and Privacy Plan

Section I.7 Internal Security:

See ScholarChip Data Security and Privacy Plan

Section II.2 Exporting of student created content:

N/A - students do not create content in the ScholarChip system

Section II.4 Review and correcting personally identifiable information:

See ScholarChip Data Security and Privacy Plan - Section II F

Section II.5 Securing student data:

TECHNOLOGY SERVICES

1050 Main Street • Roseville, CA 95678
Phone (916) 771-1645 • Fax (916) 771-1650
Laura Assem, Director of Technology

See ScholarChip Data Security and Privacy Plan, and 31-040 Information Security Policy

Section II.6 Disclosure notification:

See ScholarChip Data Security and Privacy Plan - Section IV, and 31-026 Privacy Policy

Section II.8 FERPA compliance:

See ScholarChip Data Security and Privacy Plan, and 31-026 Privacy Policy

Section III.5 How student data is protected:

See ScholarChip Data Security and Privacy Plan - Section III

SCHOLAR CHIP®
Tools for Smarter Schools™

Data Security and Privacy Plan (DSPP)

Prepared May 3, 2019 for:
Roseville City School District

Table of Contents

I. Objective and Scope

In providing Software as a Service, ScholarChip acknowledges that we have a serious obligation to help our clients protect the confidentiality of student, staff and community data in our custody. As a technology contractor for Roseville City School District ("District"), we recognize that we share certain responsibilities to protect the security and privacy of sensitive data that is collected by the District and processed by our systems. This Data Security and Privacy Plan (DSPP) outlines the administrative, technical and physical safeguards used to meet these responsibilities.

Educational data housed in ScholarChip systems, including attendance data, is protected by the Family Education Rights and Privacy Act (FERPA). Personally identifiable information (PII) of students is protected under FERPA, PPRA, COPPA and other federal, state and local regulations, including NY State Education Law section 2-d. PII belonging to parents, staff and school visitors is handled with the same care, out of respect for the privacy of all community members. ScholarChip's Privacy Policy strictly prohibits the sale of sensitive student, staff and community data under any circumstances, or the unauthorized sharing of that data with other parties. Data collected is only used for the approved purposes specified in agreements between ScholarChip and the client.

II. Data Security and Privacy Obligations

A. Relationship Between Security and Privacy

Significant overlap exists between the concepts of data security and data privacy; thus our approach to compliance has always been aimed at providing both, through multiple layers of controls designed to support our clients' policies.

B. Shared Responsibility

Privacy regulations define several distinct roles with respect to data:

Data subject/owner	the individual who is described or identified	student, staff, parent
Data controller	organization collecting the data for some defined purpose	client school or district

Data processor	provider of technology/services in support of the defined purpose	ScholarChip

Note that data privacy protection requires cooperation between the data controller (District) and the data processor (ScholarChip). In most cases, there is no direct relationship between ScholarChip and the data subject/owner. The District, as data controller, has the primary responsibility for ensuring that data is protected appropriately throughout all phases of its life cycle.

The District's role is to:

- define their business needs or purpose for collecting data
- Designate personnel responsible for data privacy matters
- Establish privacy policies and practices aligned with the defined purpose
- communicate directly with students/staff/parents regarding data collection and use
- obtain consent for data collection as appropriate
- define the conditions under which the data is no longer needed and should be purged (data retention/disposal policy)
- provide awareness training to ensure that their staff, administrators, and volunteers know how to handle sensitive data properly

ScholarChip's role is to:

- Communicate privacy objectives to internal users and clients
- provide the technical means to process data securely
- protect data while it is in our custody
- securely remove it when it is no longer needed
- provide awareness training to ensure that our employees know how to handle sensitive data properly

Note that in most cases ScholarChip does not interact directly with the data subjects; therefore it is the responsibility of the District to obtain explicit consent where appropriate. Under the FERPA "school official exception", explicit consent is not needed when data is collected for the purpose of providing the agreed-upon services, since ScholarChip is acting as an agent of the District.

C. Defining the Purpose

ScholarChip's Master License Agreement limits the "purpose" of its systems to the provision of the following broadly-defined services in support of school safety and operations:

- facilitating Student, Staff or Visitor searches/queries within the databases available to the System and displaying the results of such searches/queries in real time;
- integration or uploading data relevant to Students, Staff, Visitors and Organization into the System;
- creating reports and summaries of data relevant to Students, Staff, Visitors and Organization;
- the preparation and display of a summary intake report for your Organization;
- the provision of passes for Visitors authorized to access the Premises;
- the facilitation of record keeping and creation of reports as to individuals and/or other Visitors that may have accessed or been denied access to the Premises with such access or denial recorded by or input into the System;
- collecting and displaying information relating to the attendance, location, schedules of Students
- Collecting and recording Staff and Student observations to facilitating the administration of Student behavior management services.

Note: This is an inclusive list of services provided by the full suite of ScholarChip products. For organizations using a subset of products, the list may be more limited.

D. Allowed and Prohibited Access/Use/Disclosure

Student, staff and visitor data, whether provided to ScholarChip by the District or generated by ScholarChip through normal system operation, is only to be used for the above defined purposes. Within ScholarChip, data is only to be shared with employees who have a legitimate need to access it in connection with the agreed-upon services. All employees, whether or not they have access, receive security and privacy awareness training.

In order to provide the agreed-upon services, ScholarChip must initially receive data from PowerSchool, the District's Student Information System (SIS), and also pass some data back. Data Integration standards and processes are in place to ensure that data is transferred securely between the two systems.

- Data exchange is handled using a secure API and plugin provided by PowerSchool. Installation of and access to the plugin is managed by the District. Once the plugin is installed and enabled in the

PowerSchool Admin portal, a unique Client ID and Client Secret is generated specifically for the plugin delivered via the plugin Registration process. Technical documentation is available directly from PowerSchool.

- Student data, and staff data if applicable, is downloaded by the ScholarChip integration team using the plugin, and then imported into the ScholarChip database.
- If attendance data is to be written back to PowerSchool, this is done via the same plugin.

ScholarChip staff will only exchange information with PowerSchool to the extent necessary to provide the services described in the contract.

ScholarChip will not disclose any personally identifiable information to any other party without prior written consent of the District, unless required by statute or court order. In this case we will provide a notice of such disclosure to the District no later than the time the information is disclosed, unless providing notice of the disclosure is expressly prohibited by the statute or court order. Staff members are instructed on this through the yearly FERPA training. Any violation is met with strict disciplinary penalties, as outlined in our information security and privacy policies.

New staff orientation includes instructions on using secure mail or fmp.scholarchip.com when sending or receiving student data.

E. State/Local Data Privacy Regulations

ScholarChip is in compliance with federal and California privacy law requirements, including FERPA, COPPA, PPRA, and the Student Online Personal Information Protection Act (SOPIPA). Specific requirements include FERPA training for ScholarChip employees, adequate data protection measures, data breach notification procedures, etc.

This section outlines the District's specific student data privacy responsibilities (as a data controller) and defines ScholarChip's role (as a data processor) in meeting each of them.

F. Standard Student Data Privacy Practices

1. Restrictions on Use and Release of Student Information

Student, staff and visitor data, whether provided to ScholarChip by the District or generated by ScholarChip through normal system operation, is only to be used for the purposes defined in the Master License Agreement.

In accordance with applicable data privacy laws and ScholarChip's privacy policy, ScholarChip will not sell a student's personally identifiable information or release it for any commercial purposes.

Within ScholarChip, access to student, staff and community data is only granted to individuals who need such access to perform their job functions in connection with the specific services outlined in the service agreement.ScholarChip employees are prohibited from accessing this data for any other purpose, and are made aware of this restriction through policy and training.

In order to provide the agreed-upon services, it may be necessary to share student or staff information with subcontractors. ScholarChip maintains a third-party risk management program to ensure that such subcontractors abide by applicable data protection and security requirements.

2. Right to Review

ScholarChip acknowledges that parents have the right to inspect and review the complete contents of their child's education record. It is the Organization's responsibility to provide parents with access to this information as defined in their policies, as well as to define procedures for a parent, student, or staff member to challenge the accuracy of the information collected about them. Organization must indicate the existence of such procedures on the DSPP Worksheet;. ScholarChip will provide technical assistance as appropriate.

3. Reasonable Safeguards to Protect Confidentiality

ScholarChip acknowledges that we have a responsibility to protect the confidentiality of personally identifiable information in our custody, throughout its entire lifecycle, using reasonable administrative, technical and physical safeguards associated with industry standards and best practices. Specific protection measures in use are described in Section III of this document.

4. Addressing Privacy Concerns and Complaints

ScholarChip acknowledges that parents have the right to have complaints about possible breaches of student data addressed. Complaints should be first directed to the appropriate East Williston School District personnel as defined in their policies and the District's published PBOR.

ScholarChip's Governance Risk and Compliance (GRC) department is responsible for addressing data protection issues and concerns. Clients may contact compliance@scholarchip.com with any concerns about our privacy practices and data protection.

III. Protection of Personally Identifiable Student Information

A. ScholarChip Security Strategy - Data Protection by Design and by Default

ScholarChip systems are fully compliant with several comprehensive industry-recognized security standards. Significant overlap exists between the concepts of data security and data privacy; thus our approach to compliance has always been aimed at providing both, through multiple layers of controls designed to support our clients' defined policies.

We ensure data security using a combination of Preventive, Detective, and Organizational controls, including network architecture and configuration, software design, policies, procedures and other critical protective measures.

1. How do we decide on reasonable safeguards for the protection of student data?

ScholarChip's information security controls are based on the following industry-recognized standards and frameworks:

- NIST Cybersecurity Framework
- CIS Critical Security Controls
- SOC2 Trust Services Criteria

Our Information Security Management Committee continually reviews our existing controls to ensure that they are sufficient, using risk assessment processes recommended by the National Institute of Standards and Technology (NIST) and the Center for Internet Security (CIS)

We also rely on independent third-party assessments such as SOC2 to identify potential areas for improvement. Through a rigorous annual audit process, regular testing and constant monitoring, ScholarChip

systems are certified to meet the latest required standards governing the security of sensitive and confidential information.

Because there is never a guarantee of 100% prevention, our program also includes Response and Recovery controls.

B. Organizational Controls

1. Roles and Responsibilities

Information security/privacy responsibilities at ScholarChip are shared across multiple departments. Every effort is made to integrate security controls and processes into regular workflows and make them part of "business as usual", to maintain a continuous state of compliance with applicable regulations. The major areas of responsibility are defined as follows:

Individual or Group	Description of Responsibility
CEO/CTO	CEO/CTO - Overall responsibility for Information Security strategies and implementation Establish • system configuration standards • incident response and escalation policies Incident Response Team (must be available 24/7). Ultimate responsibility lies with CTO
Information Security Management Committee	Regular risk assessment meetings and major security/privacy-related decisions. *Committee members include CEO/CTO, President/CFO, Director of GRC and Technology Group Leader*
Director of Governance, Risk and Compliance (GRC)	Establish, document and distribute security and privacy policies Recommend appropriate organizational controls Document and distribute • system configuration standards

	• incident response and escalation policies Establish/oversee security awareness/training program; track employee participation Coordinate with HR on employee onboarding/offboarding processes related to security (employee screening, policy acknowledgement, provisioning initial systems access) Work with third party security assessors to perform annual audits of controls Conduct quarterly internal audit and review of controls Address client data security and privacy concerns, including investigation of potential breaches
GRC/Security Operations Team	Maintain asset inventory of hardware, software, and data Security Operations - Monitor, test and maintain overall network infrastructure Monitor, analyze, and distribute security alerts and information; Review security logs and follow up on exceptions Administration of user accounts on systems that handle student data; Monitor and control all access to sensitive data Ensure that all system components and software have the latest security patches installed
Technology Group Leader	Implement Secure Software Development Lifecycle for applications that handle student data Approve/sign system access requests, change control documentation
Data Integration Team	Ensure secure data handling and data integrity during integration processes

2. Policies and Procedures

We maintain a full set of security policies covering the 3 major areas of security - confidentiality, integrity and availability. Specific topics include information sensitivity/classification, privacy obligations, system configuration standards, data retention, encryption, access control, software development guidelines, security monitoring and testing, awareness and training, employee screening, incident response and business continuity.

Policies are distributed to new employees as part of onboarding, reviewed throughout the year as part of ongoing risk assessment and updated according to business/technology changes when appropriate. Updated versions are published at least annually and distributed to employees for acknowledgement.

C. Infrastructure

Data protection starts with a secure infrastructure. All critical system components are housed in ScholarChip's secure data centers, which provide assurance of physical and environmental security.

- Primary - Coresite NYC
- Secondary - Opus in Portland OR

Physical access to these data centers is limited to a very small number of ScholarChip employees.

Major components are Windows servers, primarily 2008 and 2012, which are each configured for a specific function (web server, database server, monitoring tools, etc) Servers are hardened using configuration standards based on CIS benchmarks and PCI-DSS requirements

The ScholarChip network is segmented to isolate highly sensitive data . Firewall rules are defined to explicitly allow specific types of traffic based on documented business and deny the rest by default. Rules are reviewed regularly by GRC and technical team to ensure that only the necessary traffic is being allowed.

Intrusion detection and load balancing functions are integrated into the firewall

Data in transit on our network is protected by TLS protocol.

We allow both incoming and outgoing SFTP access to service our schools and clients. All SFTP access in either direction must be with one of a pool of pre-approved "friendly" servers. (A school or client wishing to send us data or retrieve data must have credentials issued by ScholarChip.)

D. Data Storage and Protection

Sensitive data that requires special handling falls into several categories:

- PII of students - name, address, student Id number, photo - subject to various privacy regulations, including
  - NY State Education Law Section 2-d
  - Georgia Student Data Privacy, Accessibility and Transparency Act
  - PPRA
  - COPPA
  - SOPIPA
- Education records including attendance and behavioral data - subject to FERPA
- PII of staff - subject to various evolving privacy regulations

Student and staff data will be securely stored in the following ways:

Note: The table below lists data storage and protection methods for all classes of information stored and processed by all ScholarChip products and services. Not all data classes pertain to all clients. For questions relating to data storage in your specific implementation, contact your ScholarChip data integration specialist.

Storage location/medium	Data Class	Protective Controls
Oracle databases	Student PII Staff PII Attendance data Behavioral data	• Physical security (data center) • Logical access control (VPN with 2-factor authentication, Windows server login credentials, Oracle database login credentials • Data structure - data is stored in a normalized manner which minimizes the repetition of personal information. Student and staff records are assigned sequential ID numbers, and are only referenced by those ID's in other tables. This means that no Personally Identifiable Information is directly attached to educational or financial information.
NAS photo storage	Student and staff photos, class rosters and report output	• Physical security (data center) • Logical access control (VPN)
In-school devices -	student and staff IDs	• Physical security

local databases and application logs	and names, attendance data, visitor data	• Logical access control • Encryption on request
Data integration staging servers	Student data pulled from SIS in XML format	• Physical security • Logical access control (VPN with 2-factor authentication, Windows server login credentials)
SFTP server	Student contact data	• Physical security • Logical access control (VPN with 2-factor authentication, Windows server login credentials, SFTP login credentials)

E. Secure Software Development Practices

Application code vulnerabilities can result in direct or indirect exposure of sensitive information. In order to prevent this, ScholarChip applications are developed and tested in accordance with industry-recognized best practices.

- Developers receive periodic training on secure coding standards, including the use of Standard code libraries that have been vetted for security, and techniques to avoid known coding flaws such as the OWASP Top 10
- Separate Development/Test/Production environments to avoid the risk of introducing security flaws into live systems, and minimize exposure of sensitive data during development lifecycle
- Change control processes ensure that new code is tested and approved before being released
- Recently-modified code is regularly scanned for vulnerabilities

F. Logical Access Control

Logical access control is governed by the principle of least privilege. Specific users are granted the minimum access needed to perform their job functions.

In general, most ScholarChip internal staff members do not have direct access to education records, with the following exceptions:

- Our client support team has administrator-level access to the applications in order to assist client users with technical issues.
- Only specific members of technical staff can access the database directly, by remotely connecting to servers via the VPN. VPN access is only granted to those members who need it to perform their job functions, and is limited to specific servers/IP address ranges based on role. The access control list is reviewed by the GRC team on a quarterly basis to determine whether access is still needed. Accounts are modified or disabled based upon changes in job responsibilities.

1. Application Access

District staff members may be granted access to ScholarChip applications which allow them to view and/or modify student PII and education records. Such access is governed by a system of Roles and Permissions that define what a specific user can see and do within the application. Responsibility for managing such access is shared between ScholarChip and the District.

Application user accounts may be created by ScholarChip staff during the implementation phase. Once the system is in production use, accounts may also be created by District staff members who have Administrator privileges. This allows the District to determine appropriate access based on staff responsibilities and “need to know”.

In order to prevent unauthorized application access:

- Passwords are stored encrypted with a one way hash.
- Temporary passwords are assigned when a management site Administrator or Developer creates a login or resets a password for a user at a lower level. These temporary passwords must be unique for each user.
- Users must change password upon first login.
- Accounts are locked after 6 invalid login attempts.
- Passwords cannot be retrieved, only changed to new passwords.
- Passwords are made to expire after 30 days of non-use.

2. Tech Staff Access

All direct access to ScholarChip system components is required to go through our VPN.

Only a small group of VPN administrators can create new VPN accounts or reset expired passwords.

Management approval is required, and VPN users must have completed security training and acknowledged security policies prior to receiving access.

Access to VPN is authenticated via a 2-factor authentication process.

Access to all servers is granted according to the principle of least privilege; that is, an individual

Is granted only the minimum privileges necessary to do their assigned job.

All members of the ScholarChip development team require administrative access to the systems they develop and support. Developers have both privileged and non-privileged accounts where

feasible, and only use the privileged accounts when performing specific functions that actually require administrative access, such as:

- Running an Application as an Administrator
- Changes to system-wide settings
- Installing and uninstalling applications, device drivers
- Configuring Windows Update
- Adding/removing/changing user accounts
- Running Task Scheduler
- Restoring backed-up system files
- Viewing or changing another user’s folders and files

Access is reviewed annually or when personnel changes take place

Non-development staff will be granted privileges on an as-needed basis. In general, only some members of the Help Desk, Implementation and GRC departments may require administrative access to certain servers; other departments do not require such access. Access requirements must be documented and approved by management before access is granted.

Poorly chosen passwords may result in the compromise of ScholarChip's entire corporate network. As such, all ScholarChip employees (including contractors and vendors with access to ScholarChip systems) are

responsible for taking appropriate steps to select and secure their passwords. Periodic security awareness training outlines current “best practice” recommendations for managing passwords.

G. System monitoring and testing

ScholarChip continuously monitors its systems for unauthorized activity that may result in the exposure of sensitive data.

Daily log reviews are the responsibility of the GRC department. The purpose of the daily log monitoring process is to document unusual occurrences in order to spot potential system security and operational problems, including both internal and external threats. Logs are aggregated using centralized audit logging mechanisms (syslog, EventTracker) to allow for some automation of the review process, as well as correlation of events from different sources. Critical issues are picked up by semaphore alerts on a real-time basis.

The following are some of the components monitored by the GRC team on a daily basis:

- Pfsense Firewalls/IDS (Snort) - alerts are reviewed daily using a combination of automated and manual methods. IP addresses with unusual activity may be blacklisted, depending on country of origin and reputation.
- File Integrity Monitoring (OSSEC) - this alerts us to unexpected file changes on Windows servers that support the infrastructure (database servers, web application servers and monitoring servers), which could be an indicator of compromise
- Anti-virus (Bitdefender)
- Logical access controls (VPN and Windows logins and account changes)
- Installation of software on endpoints - Our network asset inventory tool alerts us to installation of new software on endpoints; unauthorized applications are evaluated to determine risk level and removed if deemed unacceptable
- Cloud application usage and data sharing - we use a cloud access/SaaS monitoring solution to detect and remediate instances of employees sharing sensitive information in unauthorized ways (either deliberately or inadvertently)

Vulnerability scanning and penetration testing are also performed regularly. Results are reviewed by GRC and technical teams and any issues are remediated in a timely manner to reduce the potential for exploit of system vulnerabilities from the outside.

IV. Breach notification requirements

Should ScholarChip become aware of any unauthorized release of student data, in violation of applicable privacy laws, the parents' bill of rights, and/or binding contractual obligations relating to data privacy and security, we will notify the Organization's designated privacy official in the most expedient way possible and without unreasonable delay.

If there is valid reason to suspect a breach (i.e., clients report fraudulent activity on their accounts, or we see signs that someone has gained unauthorized remote or physical access to the data center), ScholarChip incident response team will:

- check for common indicators of compromise to determine whether or not a breach has actually occurred.
- Notify CTO, GRC, and application owners of findings.
- Conduct additional research as necessary to determine the extent of impact.

If it is determined that a breach has occurred, system(s) or system component(s) may need to be taken offline until they can be locked down with additional security measures (change passwords and certificates, update firewall settings, etc.) An official statement will be issued to clients, summarizing our findings and providing an estimated time frame for service restoration.

V. Data Retention and Disposal

Student and staff data will only be stored as long as the District legitimately needs it. ScholarChip's data architecture makes it straightforward to remove an individual's data at the request of the data controller (client) if it is no longer needed for a legitimate business purpose. Clients must define their data retention criteria on the accompanying DSPP Worksheet (i.e., delete student records "X" years after graduation.)

What happens to the student and staff data upon contract termination or expiration?

Unless otherwise agreed-upon by the Parties in writing, ScholarChip shall remove or overwrite all Data from ScholarChip's systems following the effective date of termination or cancellation, in accordance with ScholarChip's standard procedures.

SCHOLARCHIP INFORMATION SENSITIVITY POLICY (PRIVACY POLICY)

1.0 OVERVIEW AND PURPOSE

Privacy is Paramount

Depending on the services ScholarChip provides, we gather identification data every day about students, teachers, visitors, vendors, or anyone who goes into a school building, from schools and universities across the country. We are also entrusted with sensitive account and transaction data gathered by our Higher Education financial applications.

The Federal Information Security Management Act (FISMA), which is part of the Electronic Government Act of 2002, defines a comprehensive framework to protect information, operations and assets against natural or man-made threats. These guidelines help administrators navigate data security issues, such as keeping student data private. ScholarChip is dedicated to following these important guidelines, as well as many other data security guidelines, to keep our clients' information private and safe.

Why We Gather Data

ScholarChip is the largest provider of smart ID cards for K12; these cards are the key to the services ScholarChip provides, like building, classroom, event, and bus attendance; secure door access; visitor management services; cafeteria POS; and even behavior and discipline tracking. These cards are coded with a unique ID number that is assigned to one individual; they are inherently secure because they provide an encrypted digital identity. It's the back-end computer that maintains all the information on that person.

The data we gather provides access to over 100 reports when a school has full program implementation. These reports, based on the materials we gather, provides identifiable, actionable information for school districts. The detail captured helps keep schools safer, and provides a host of information that can be analyzed and used to improve student performance as well as administrative effectiveness.

Type of Data Collected

Student data is personal information gathered that includes name, address, names of parents or guardians, date of birth, grades, attendance, disciplinary records, eligibility for lunch programs, special needs, and other information necessary for basic administration and instruction. On the Higher Education level, student loan, bank and credit card account data may also be collected.

Teacher data includes name, address, phone numbers, in case of emergency contacts, etc.; volunteer or visitor data is scanned from a driver's license and saved in a school's database.

Sharing the Data

ScholarChip takes the security and privacy of student data very seriously. We never sell our data. We sometimes share information for marketing purposes, but only school-wide trends, and we receive prior written authority from school district(s) being cited and/or the person(s) being quoted.

ScholarChip's Management Portals serve data to all users at the appropriate level. School users have access only to their school's data; central office or district administrative personnel have access to all data. Additional access levels can also be supported.

2.0 SCOPE

Understanding your Responsibilities

The Compliance Officer is responsible for implementing and monitoring data protection guidelines and privacy practices at ScholarChip. All employees have a responsibility to understand these guidelines and to follow the recommended practices to the best of their ability.

This Information Sensitivity/Privacy Policy is intended to help employees determine what information can be disclosed to non-employees, as well as the relative sensitivity of information that should not be disclosed outside of ScholarChip without proper authorization.

The information covered in these guidelines includes, but is not limited to, information that is either stored or shared via any means. This includes: electronic information, information on paper, and information shared orally or visually (such as telephone and video conferencing).

All employees should familiarize themselves with the information labeling and handling guidelines at the end of this document. It should be noted that the sensitivity level definitions were created as guidelines and to emphasize common sense steps that you can take to protect ScholarChip Confidential information (e.g., ScholarChip Confidential information should not be left unattended in conference rooms).

Please Note: The impact of these guidelines on daily activity should be minimal.

Questions about the proper classification of a specific piece of information should be addressed to your manager. Questions about these guidelines should be addressed to the Compliance Officer or Chief Security Officer (CSO).

All ScholarChip information is categorized into two main classifications:

- ScholarChip Public
- ScholarChip Confidential

ScholarChip Public information is information that is public knowledge and can be freely be given to anyone without any possible damage to ScholarChip.

ScholarChip Confidential contains all other information. It should be understood that some types of information are more sensitive than others, and need to be protected in a more secure manner. Included is information that should be protected very closely, such as credit card data, student records, etc. Also included in ScholarChip

Confidential is information that is less critical, such as general corporate information, HR information, etc., which does not require as stringent a degree of protection.

ScholarChip personnel are expected to use common sense judgment in securing ScholarChip Confidential information to the proper extent. If an employee is uncertain of the sensitivity of a particular piece of information, he/she should contact their manager or the Compliance Officer. Any and all third parties handling or processing ScholarChip Confidential information are bound by the terms of this privacy policy.

3.0 POLICY

PROTECTING COMPANY AND CLIENT INFORMATION

All access to computer networks, including remote access, is granted to employees on a case by case basis, according to business needs. Employees must do their utmost to protect such access and to cease any access once employment is terminated.

Source code and other proprietary information, including designs and system architectures, are solely the property of the company and may not be shared with any outside agencies.

Protecting our company's information is the responsibility of every employee, and we all share a common interest in making sure it is not improperly or accidentally disclosed. This also includes sensitive client information, such as credit card numbers, SSNs, student records, visitor information, and other personally identifiable information. Employees should take care to access and disclose only that data which is needed for legitimate business purposes. Do not discuss the company's confidential business with anyone who does not work for us. You may be required to sign a (non-compete) (nondisclosure) agreement as a condition of your employment, in accordance with State and Federal law.

The Sensitivity Guidelines below provide details on how to protect information at varying sensitivity levels. Use these guidelines as a reference only, as more or less stringent measures of protection may be required depending upon the circumstances and the nature of the information in question, and the particular privacy policies of specific client schools.

3.1 MINIMAL SENSITIVITY

Includes: General corporate information; some HR and technical information

Marking guidelines for information in hardcopy or electronic form: *Marking is at the discretion of the owner or custodian of the information. If marking is desired, the words "ScholarChip Confidential" may be written or designated in a conspicuous place on or in the information in question. Even if no marking is present, ScholarChip information is presumed to be "ScholarChip Confidential" unless expressly determined to be ScholarChip Public information by a ScholarChip employee with authority to do so.*

Access: All ScholarChip employees and contractors; however, to minimize exposure, it is recommended that distribution is limited to people with a business need to know, as determined by the information owner.

Distribution within ScholarChip: Use standard company-approved electronic mail and electronic file transmission methods.

Distribution outside of ScholarChip internal mail: U.S. mail and other public or private carriers, approved electronic mail and electronic file transmission methods.

Electronic distribution: No restrictions except that it be sent to only approved recipients. (Use of secure methods is optional for this level.)

Storage: Keep from view of unauthorized people; erase whiteboards, do not leave in view on tabletop. Machines should be administered with security in mind. Protect from loss; electronic information should have individual access controls where possible and appropriate.

Disposal/Destruction: Outdated paper copies should be shredded; electronic data should be expunged. Reliably erase or physically destroy media.

3.2 MORE SENSITIVE

Includes: Student, teacher and visitor demographic data including address and phone number; business, some technical, and most HR information

NOTE: Information classified at this level is not to be sold to a third party under any circumstances.

Marking guidelines for information in hardcopy or electronic form: *As the sensitivity level of the information increases, you may, in addition to marking the information "ScholarChip Confidential", wish to label the information "Internal Use ONLY" or other similar labels to denote a more sensitive level of information. However, marking is discretionary at all times.*

Access: ScholarChip employees who have a business need to know. This includes application developers, Help Desk and Implementation staff as part of normal business duties, and other employees for specific cases, at the discretion of the CTO or Compliance. . Do not share outside of ScholarChip without an appropriate confidentiality agreement.

Distribution within ScholarChip: Use company-approved ***secure*** electronic mail and electronic file transmission methods. Do not share in any cloud-based collaboration tools.

Distribution outside of ScholarChip internal mail: Sent via U.S. mail or approved private carriers.

Electronic distribution: No restrictions to approved recipients within ScholarChip, but should be encrypted in accordance with the *Encryption Policy* or sent via a private link to approved recipients outside of ScholarChip premises**Storage:** Electronic information at this sensitivity level should be password-protected.

Disposal/Destruction: Outdated paper copies should be shredded; electronic data should be expunged. Reliably erase or physically destroy media.

3.2.1 - NOTIFICATION OF FAMILY EDUCATIONAL RIGHTS AND PRIVACY ACT (FERPA)

ScholarChip is not a school or university; however, ScholarChip systems may contain certain educational data which falls under this classification and is protected by the Family Education Rights and Privacy Act (FERPA). As a provider of technology used in essential school operations, ScholarChip falls under the "school official" exception for specific FERPA requirements. FERPA affords students certain rights with respect to their education records, as follows:

(1) The right to inspect and review the student's education records within 45 days of the day the organization receives a request for access. Students should submit to the appropriate official written requests that identify the record(s) they wish to inspect. The university official will make arrangements for access and notify the student of the time and place where the records may be inspected. If the records are not maintained by the university official to whom the request was submitted, that official shall advise the student of the correct official to whom the request should be addressed.

(**2) The right to request the amendment of the student's education records that the student believes are inaccurate or misleading.** Students may ask the organization to amend an educational record that they believe is inaccurate or misleading. They should write the official responsible for the record, clearly identify the part of the record they want changed and specify why it is inaccurate or misleading. If the organization decides not to amend the record as requested by the student, the organization will notify the student of the decision and advise the student of his or her right to a hearing regarding the request for amendment. Additional information regarding hearing procedures will be provided to the student when notified of the right to a hearing.

(3) The right to consent to disclosures of personally identifiable information contained in the student's education records, except to the extent that FERPA authorizes disclosure without consent. One exception which permits disclosure without consent is a disclosure to school officials with legitimate educational interests. A "school official" is a person employed by the organization in an administrative, supervisory, academic or research, or support staff position (including law enforcement unit personnel and health staff); a person or company with whom the university has contracted (such as an attorney, auditor or collection agent); a person serving on the Board of Governors; or a student serving on an official committee, such as a disciplinary or grievance committee, or assisting another school official in performing his or her tasks. A school official has a legitimate educational interest if the official needs to review an education record in order to fulfill his or her professional responsibility.

(4) The right to file a complaint with the U.S. Department of Education concerning alleged failures by ScholarChip to comply with the requirements of FERPA. The name and address of the office that administers FERPA are: Family Policy Compliance Office, U.S. Department of Education, 600 Independence Avenue SW, Washington, DC 20202-4605.

3.2.2 – POSTED PRIVACY STATEMENT

The following statement is posted on ScholarChip websites to inform users of our Data Disclosure policy:

ScholarChip's Commitment to Privacy
Your privacy is important to us. To better protect your privacy we provide this notice explaining our online information practices and the choices you can make about the way your information is collected and used.

The Information We Collect
This notice applies to all information collected or submitted *on https://payserv.scholarchip.com and https://paypage.scholarchip.com** website. In order to process your transaction and allow you to manage your account information and transaction history, personal information collected may include name, address, phone number, email address, credit / debit card and/or bank account information. We do not sell or share this identifiable information with anyone for any purpose. Our sole purpose is to collect this information to complete your transaction. The information collected is shared with parties only to the extent necessary to complete your transaction.

ScholarChip's Commitment To Data Security
We are committed to safeguarding your security. To guarantee that the information submitted on our website remains absolutely secure and confidential, we use industry-standard hardware and software in combination with authentication and certification by third parties and we also encrypt all sensitive information and financial data. We also conform to the highest levels of the Payment Card Industry (PCI) security standards

* substitute appropriate site name(s) here

3.3 MOST SENSITIVE

Includes: Credit card data; SSN's; source code; marketing, operational, financial, and technical information integral to the success of our company.

NOTE: Information classified at this level is not to be sold to a third party under any circumstances. *Credit card data protection measures must always comply with the latest PCI-DSS requirements (version 3.2 at the time of this revision).*

Marking guidelines for information in hardcopy or electronic form: *To indicate that this type of ScholarChip Confidential information is very sensitive, you should ALWAYS label the information, "ScholarChip Confidential" and "Internal Use ONLY". Users should be aware that this information is very sensitive and must be protected as such.*

Access: Only those ScholarChip employees designated with explicit approved access (management signature required.)

Distribution within ScholarChip: Delivered directly - signature required, envelopes stamped confidential, or approved ***secure*** electronic file transmission methods. Do not share in cloud-based collaboration tools.

Distribution outside of ScholarChip internal mail: Delivered directly; signature required; approved private carriers.

Electronic distribution: All information at this sensitivity level must be strongly encrypted in accordance with the *Encryption Policy* and PCI Requirement 4.1, and must not be sent by end-user messaging technologies (text or instant messaging) in accordance with PCI Requirement 4.2.

Storage: Electronic information at this sensitivity level MUST be password-protected. Physical security is generally used, and information should be stored in a physically secured computer.

Disposal/Destruction: Outdated paper copies MUST be shredded; electronic data MUST be expunged. Reliably erase or physically destroy media.

4.0 ENFORCEMENT

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 DEFINITIONS

Expunge - To reliably erase or expunge data on a PC or Mac you must use a separate program to overwrite data. Otherwise, the PC or Mac's normal erasure routine keeps the data intact until overwritten.

Physical Security - Physical security means either having actual possession of a computer at all times, or locking the computer in an unusable state to an object that is immovable. Methods of accomplishing this include having a special key to unlock the computer so it can be used, thereby ensuring that the computer cannot be simply rebooted to get around the protection. If it is a laptop or other portable computer, never leave it alone in a conference room, hotel room or on an airplane seat, etc. Make arrangements to lock the device in a hotel safe, or take it with you. In the office, always use a lockdown cable. When leaving the office for the day, secure the laptop and any other sensitive material in a locked drawer or cabinet.

Private Link - A Private Link is an electronic communications path that ScholarChip has control over its entire distance. For example, all ScholarChip networks are connected via a private link. A computer with modem connected via a standard land line (not cell phone) to another computer have established a private link.

6.0 REVISION HISTORY

4/16/10 – DJH - Policy created

5/13/10 – DJH - Minor corrections

7/14/10 – DJH - Formatting changes

2/1/13 - DJH - Annual Policy Review 2013 – Changed document name to identify this as privacy policy; sections 3.2 and 3.3 – modified classification definitions, added statement prohibiting sale of sensitive information; section 3.2 – added FERPA statement; section 3.3 – added PCI requirements to Electronic Distribution guidelines; minor formatting changes; changed version number to 2.0

3/6/15 – TM – Annual Policy Review 2015 - Section 3.3: Updated PCI version to 3.0. Corrected phrasing of internal distribution to "Delivered directly with signature required"

6/3/15 – DJH – review in response to an employee incident

- Section 2.0 – added last sentence regarding third parties/subcontractors
- section 3.0 - added paragraphs on Protecting Company Information (from Employee Handbook)

- added Section 3.2.2- Posted Privacy Statement

8/18/16 – DJH – sections 3.1-3.3 – added guidance on when to use newly-implemented secure email and file transfer methods rather than standard methods

2/2/17 – DJH – incorporated language from proposed K-12 Privacy Policy to create one unified policy for the entire organization.

9/15/17 – DJH – modified to meet SOC2 privacy requirements

- page 2 – added Understanding Your Responsibilities heading and a paragraph naming Compliance Officer as responsible for implementation and monitoring of privacy practices. Moved these, and the next 3 paragraphs, to Section 2.0
- section 3.0 – changed heading to "PROTECTING COMPANY AND CLIENT INFORMATION"; added "visitor information" to list of sensitive data types, added " and the particular privacy policies of specific client schools" to last sentence.
- Sections 3.1-3.3 – made Access guidelines for each data classification more specific
- Section 3.2.1 – added sentence about "school official" exception for FERPA
- Section 3.3 – updated PCI-DSS version
- Updated revision date and version number

3/7/18 – Annual Review – DJH

- Section 2.0 – changed "encouraged" to "expected"
- Section 3.2 – added requirement for confidentiality agreement
- Sections 3.2 and 3.3 – added restriction on sharing in cloud-based collaboration tools
- Modified version number and revision date

SCHOLARCHIP

INFORMATION SECURITY POLICY

MARCH 2018 VERSION 3.7

SCHOLAR CHIP

TABLE OF CONTENTS

ABOUT THIS DOCUMENT

To safeguard ScholarChip's information technology resources and to protect the confidentiality of data, adequate security measures must be taken. This Information Security Policy reflects ScholarChip's commitment to comply with required standards governing the security of sensitive and confidential information.

Inappropriate exposures of confidential and/or sensitive information, loss of data and inappropriate use of computer networks and systems can be minimized by complying with reasonable standards (such as the Payment Card Industry Data Security Standard), attending to the proper design and control of information systems, and applying sanctions when violations of this security policy occur.

Security is the responsibility of everyone who uses ScholarChip's information technology resources. It is the responsibility of employees, contractors, business partners, and agents of ScholarChip. *Each should become familiar with this policy's provisions and the importance of adhering to it when using ScholarChip's computers, networks, data and other information resources. Each is responsible for reporting any suspected breaches of its terms*. As such, all information technology resource users are expected to adhere to all requirements outlined in this Information Security Policy.

This document contains the ScholarChip information security policies. Detailed standards and processes that support this policy are described in associated numbered documents, which can all be found on our management site and internal wiki. This document is for internal use only and is not to be distributed outside of the organization unless authorized by the Compliance department and/or the CTO.

PURPOSE / SCOPE

The primary purpose of this security policy is to establish rules to ensure the protection of confidential and/or sensitive information stored or transmitted electronically and to ensure protection of ScholarChip's information technology resources. The policy assigns responsibility and provides guidelines to protect ScholarChip's systems and data against misuse and/or loss.

This security policy applies to all users of computer systems, centrally managed computer systems, or computers that are authorized to connect to ScholarChip's data network. It may apply to users of information services operated or administered by ScholarChip (depending on access to sensitive data, etc.). Individuals working for institutions affiliated with ScholarChip are subject to these same definitions and rules when they are using ScholarChip's information technology resources.

This security policy applies to all aspects of information technology resource security including, but not limited to, accidental or unauthorized destruction, disclosure or modification of hardware, software, networks and/or data.

This security policy has been written to specifically address data security requirements established by the Payment Card Industry. Credit card data stored, processed or transmitted by ScholarChip must be protected and security controls must conform to the Payment Card Industry Data Security Standard (PCI

DSS). Sensitive credit card data is defined as the Primary Account Number (PAN), Card Validation Code (CVC, CVV2, CVC2), and any form of magnetic stripe data from the card (Track 1, Track 2).

SECURITY POLICY OWNERSHIP AND RESPONSIBILITIES

It is the responsibility of the custodians of this security policy to publish and disseminate these policies to all relevant ScholarChip system users (including vendors, contractors, and business partners). Also, the custodians must see that the security policy addresses and complies with all standards ScholarChip is required to follow (such as the PCI DSS, NIST, SOC2, etc). This policy document will also be reviewed at least annually by the custodians (and any relevant data owners) and updated as needed to reflect changes to business objectives or the risk environment.

Questions or comments about this policy should be directed to the custodians of this policy as detailed in the table below:

Table 1 – Security Policy Custodians

Name	Title	Phone	E-Mail Address
Maged Atiya	CTO/CSO	x101	matiya@scholarchip.com
Donna Harrigan	Compliance Officer	X117	dharrigan@scholarchip.com

Table 2 - Revision History

Version	Date	Author	Description of Change
1.0	4/1/2010	Donna Harrigan	Security Policy draft created
1.0	5/17/2010	Donna Harrigan	First version finalized for publishing; all revisions after this point will require a new document version number
1.0	6/14/2010	Donna Harrigan	Made all changes requested by SecurityMetrics QSA Bruce Bogdan during PCI audit; reset version to 1.0
2.0	5/2/2011	Donna Harrigan	Annual review
2.1	6/16/2011	Donna Harrigan	Made all changes requested by SecurityMetrics QSA Brandon Benson during PCI audit: - Specifically prohibit printing of card data (p 21) - Require authorization for disclosure of private IP addresses (p 8)
3.0	5/1/2012	Donna Harrigan	Annual review; some re-wording for FISMA
3.1	7/10/12	Donna Harrigan	Added CTO/CSO responsibility to Appendix A; modified section 6.6 p 18 (changed from Acunetix to

Version	Date	Author	Description of Change
			NetSparker)
3.2	4/15/13	Donna Harrigan	Updated section 6.4 on change control tracking; added cross-references to separate policy and procedures
3.3	6/10/14	Donna Harrigan	Annual review; removed references to F5 and to obsolete documents; updated anti-virus info for Requirement 5 on page 15; added reference to SCMM policy; updated version number and revision date.
3.4	5/28/15	Donna Harrigan	Annual review; removed SAS70 and added SSAE16 and FISMA to statement about security assessments at end of section 1.3; edited section 4.2 to address new PCI requirement to elimnate SSL in favor of TLS 1.2; updated version number and revision date.
3.5	4/5/16-4/29/16	Donna Harrigan, Tim Mui	Annual review • Roles and Responsiblities chart (p 33 – added Donna Harrigan to "Administration of User Accounts", Tim Mui to monitoring and reviewing of alerts and logs • Section 1.1 - removed reference to Firewall Protocols document 31-240 which is no longer used; • section 6.4 - removed reference to App Change Approval Form 31-620, (no longer used) and changed wording to reflect the submission of app change requests via email or "Project"; • section 6.6 – removed reference to Netsparker; added cross-reference to doc 31-923 • section 7.1 - added statement about using email as an alternate form of documentation for access requests. • Section 12.3 – changed "Employees working in the cardholder environment" to "Employees working with sensitive data" • Section 12.4 – changed "employees who will

Version	Date	Author	Description of Change
			have access to cardholder data" to "employees who will have access to sensitive data" • Section 12.6 – changed 12.9 to 12.10 to correspond with numbering in PCI-DSS v3.1, removed specific sub-requirement numbers after each bullet point
3.6	3/15/17-4/22/17	Donna Harrigan	• Page 4 – revised About This Document section to state that this document is "not to be distributed *outside of the organization unless authorized by the Compliance department and/or the CTO*" • Section 1.3 – added language about disclosing network information for client due diligence requests • Added section 3.4 on "Applying PCI Standards to Other Sensitive Data" to broaden scope of policy • Sections 6.1, 10.1, 11.4 – removed references to doc 31-520 (no longer used in its current form – will be incorporated into 31-4000 SCPP and/or published on Google Drive) • Section 12.5 – replaced references to "cardholder data" with "sensitive data" to broaden scope of policy • Page 32 - Updated Roles/Responsibilities matrix
3.7	3/5/18	Donna Harrigan	• Revised Roles/Responsibilities matrix to reflect recent reorganization • Revised wording of Purpose/Scope version to enhance clarity with regard to PCI • Section 2.3 – added note about TLS 1.2 requirement • Section 4.2 – expanded scope beyond card

Version	Date	Author	Description of Change
			data; added cross-ref to Doc 31-026 • Section 5.1 - made more generic to allow for migration to new anti-virus solutions as deemed appropriate; added cross-ref to new Doc 31-6060 • Section 6.2 – expanded scope beyond system administrators and card data • Section 6.3 – added cross-ref to doc 31-923 • Section 7.1 – made approval requirement more generic based on recent reorganization • Section 8.5 – changed cross-ref for password standards from 31-023 Password Policy to 31-4821 Access Control Policy • Section 9.0 – added cross-ref to Doc 31-5980 • Section 9.4 – changed electronic filing instructions from “your workstation” to “a secure location” • Section 11.1 – added cross-ref to Doc 31-5981 • Section 11.3 – added requirement for segmentation testing and cross-ref to scope and rules of engagement • Section 11.4 – moved 31-4000 cross-ref to more general intro in section 11.0 • Section 12.3 – modified frequency of distribution of policy updates • Section 12.4 – added note about additional required screening • Section 12.5 – added cross-ref to Doc 31-5880 Vendor Management

BUILD AND MAINTAIN A SECURE NETWORK INFRASTRUCTURE

In order to protect sensitive and/or confidential data, including cardholder data, it is critical to design and maintain a secure network infrastructure where this data may be stored, processed, or transmitted. The following polices cover the network infrastructure (hardware such as firewalls, routers, and switches) as well as requirements for the secure configuration of all system components (network hardware, servers, workstations, etc.).

1.0 FIREWALL CONFIGURATION TO PROTECT SENSITIVE DATA

Firewalls are computer devices that control computer traffic allowed between ScholarChip's network (internal) and untrusted networks (external), as well as traffic into and out of more sensitive areas within a company's internal trusted network.

A firewall examines all network traffic and blocks those transmissions that do not meet ScholarChip's specified security criteria.

All systems must be protected from unauthorized access from untrusted networks, whether entering the system via the Internet as e-commerce, employees' Internet access through desktop browsers, employees' e-mail access, dedicated connections such as business to business connections, via wireless networks, from less secure to more secure network segments on an internal corporate network, or via other sources. Often, seemingly insignificant paths to and from untrusted networks can provide unprotected pathways into key systems. Firewalls are a key protection mechanism for any computer network.

1.1 FIREWALL/ROUTER CONFIGURATION DOCUMENTATION

ScholarChip's firewall/router configuration standards and change management process are outlined in Document 31-460, titled ***ScholarChip Firewall Policy and Documentation***. This document and the system Network Diagram must be kept up-to-date in compliance with PCI-DSS Requirement 1, and must always include the following:

- Process for firewall/router change management and testing of inbound and outbound network connections.
- Roles and responsibilities for logical management of the firewalls/routers.
- Detailed list of inbound and outbound services, protocols, and ports required for daily business; description and justification for use of the required services, protocols, and ports on all firewall interfaces.
- Detailed list of all insecure or risky services, protocols and ports used, the reasons for using those services, protocols and ports, and the security features necessary to protect these services/protocols.

1.2 RESTRICT CONNECTIONS WITH THE CARDHOLDER DATA ENVIRONMENT

ScholarChip will restrict connections from untrusted network segments to system components within the cardholder data environment by doing the following:

Note: An "untrusted network" is any network that is external to the networks belonging to ScholarChip under review, and/or which is out of ScholarChip's ability to control or manage (e.g. the Internet, connected vendor networks, public wireless networks). An "untrusted network may also include lower security ScholarChip networks that are used for normal business purposes but are not used for the storing, processing, or transmitting of sensitive data (e.g. corporate office networks).

- Firewall rules must limit all inbound and outbound traffic to/from the cardholder data network to only that which is necessary for business.
- Firewall and router running configurations must be secure and synchronized—for example, running configuration files (used for normal running of the firewall/routers) and start-up configuration files (used when machines are re-booted) must have the same, secure configurations.
- When wireless networking is used, a firewall must exist between any wireless network and the cardholder data environment. Firewall rules must prohibit insecure traffic and restrict traffic from the wireless segment to only that which is necessary for business.

1.3 PROHIBIT DIRECT PUBLIC ACCESS TO THE CARDHOLDER DATA ENVIRONMENT

ScholarChip will prohibit direct public access between the Internet and any system component in the cardholder data environment. Details are outlined in Document 31-460, titled ***ScholarChip Firewall Policy and Documentation.***

The above mentioned documents must be reviewed quarterly and revised as necessary, and must always meet the following criteria, in order to satisfy PCI-DSS Requirement 1.3 and all its sub-requirements:

- Create a DMZ to limit inbound and outbound traffic to only protocols that are necessary for the cardholder data environment.
- Limit all inbound traffic from the Internet to addresses within a DMZ.
- Direct network routes are prohibited (inbound or outbound) between the Internet and the segment of the cardholder data network where sensitive card data is persisted.
- Do not allow internal IP addresses (e.g. – RFC 1918 address ranges) to pass from the Internet into the cardholder data network.
- Use firewall hardware that implements stateful inspection, also known as dynamic packet filtering. (That is, only "established" connections are allowed into the network.)

- All stored cardholder data must be kept within an internal network zone segmented from the DMZ and all other network segments with direct Internet access.
- All internal network addresses (10.0.0.0) are NATed by the firewall to any external network. This is true for all web servers. It is also true for any network access by non-web server machines (such as FTP or database machines). This is automatically enforced by our network topology and rules. The easiest way to verify this is to browse to the site:

  http://www.whatismyip.com.

Internal IP addresses and routing information must not be disclosed to any external parties, except for the purposes of security assessment (PCI, SSAE16, FISMA, etc.) and client due diligence. Management approval is required for disclosure of this information to auditors and/or clients.

1.4 PERSONAL FIREWALL REQUIRED ON MOBILE COMPUTERS

ScholarChip does not allow any mobile devices as part of the network. Any device such as a laptop is considered insecure and can only access the network in a standard fashion for insecure devices, such as via the web interface or VPN/SSL. However, if this restriction is ever lifted, the following will be required, in order to comply with PCI-DSS Requirement 1.4:

- Personal firewalls must be installed and active on all mobile and/or employee-owned computers with direct connectivity to the Internet (for example, laptops used by employees), and which are used to directly access the cardholder data network.

- Personal firewall software is to be configured by ScholarChip to specific standards and configurations should not be alterable by mobile computer users.

2.0 CHANGE VENDOR SUPPLIED DEFAULTS

System components used in sensitive networks often will come with default vendor settings (usernames, passwords, configuration settings, etc.). ScholarChip's general policy is to always change vendor-supplied defaults for system passwords or other security parameters before systems are installed in the secure network environment (cardholder data network).

Individuals with malicious intent (external and internal to a company) often use vendor default passwords and other vendor default settings to compromise systems. These passwords and settings are well known by hacker communities and are easily determined via public information.

2.1 CHANGE VENDOR SUPPLIED DEFAULTS

- All vendor-supplied defaults MUST be changed on all system components before being used in the cardholder data network. (Examples include: passwords, simple network management

protocol (SNMP) community strings, and elimination of unnecessary accounts, etc.) (PCI-DSS Requirement 2.1)

- All default settings for wireless environments (equipment) connected to the cardholder data environment or transmitting cardholder data MUST be changed before enabling the wireless system for production use. (PCI-DSS Requirement 2.1.1)
- All wireless devices MUST be configured to support strong encryption technologies for both authentication to the network and transmission of data. (PCI-DSS Requirement 2.1.1)

2.2 SYSTEM HARDENING AND STANDARD CONFIGURATION OF DEVICES

Documented system configuration standards must be developed and followed for all system components. Details can be found in Document # 31-805, ***System Hardening Guidelines***.

These system configuration standards must address all known security vulnerabilities for systems used in the card network. Standards must be consistent with either SANS, NIST, CIS, or similar security industry standards and address all PCI configuration requirements (e.g. password requirements, log settings, File Integrity Monitoring, Anti-virus software, etc.).

Documented system configuration standards must be applied when new systems used in the card network are configured and before systems are placed into production.

General Configuration Requirements:

- Only one primary function is to be implemented per server. (PCI-DSS Requirement 2.2.1)
- Unnecessary services or protocols are not to be enabled.
- If any insecure protocols are used, they must be justified and documented as to the appropriate use of the service. (PCI-DSS Requirement 2.2.2)
- Security parameter settings for all devices in the card network must be documented in the system configuration standards. (PCI-DSS Requirement 2.2.3)
- All unnecessary functionality (i.e. scripts, drivers, features, subsystems, file systems, and unnecessary web servers) must be removed from system components in the cardholder network. (PCI-DSS Requirement 2.2.4)
- All required functionality must be documented in the system configuration standards. These functions must support secure configuration, and only documented functionality may be present on systems in the card network. (PCI-DSS Requirement 2.2.4)

2.3 USE SECURE PROTOCOLS FOR NON-CONSOLE ACCESS

- Strong cryptography must be used for any non-console and/or web-based management interface used for administration of systems and/or system components. (*Use technologies such as SSH, VPN, or SSL/TLS* for web-based management and other non-console administrative access.)* (PCI-DSS Requirement 2.3)

  For further details, see Document #31-160, ***Securing Remote Administrative Access***.

*Note – PCI-DSS version 3.2 requires the use of TLS protocol 1.2 instead of SSL, but the certificates are still commonly referred to as SSL certificates.

PROTECT SENSITIVE DATA

Sensitive and/or confidential data (e.g. – Cardholder Data: PAN and sensitive authentication data) must be protected when stored and when it is in transit over public (or un-trusted) networks. Strong industry standard encryption methodologies must be used to protect data stored on hard drives, removable media, backups, etc. The following policies ensure proper encryption of stored data and data in transit over open, public networks.

3.0 PROTECT STORED DATA

Protection methods such as encryption, truncation, masking, and hashing are critical components of sensitive data protection. If an intruder circumvents other network security controls and gains access to encrypted data, without the proper cryptographic keys, the data is unreadable and unusable. Credit card data has many sensitive components, including the Primary Account Number (PAN), magnetic stripe authentication data (Track1, Track2), Card Verification Code (CVC), and the Personal Identification Number (PIN), etc. The following policies address the treatment of sensitive credit card data.

3.1 RETENTION AND DISPOSAL OF SENSITIVE CREDIT CARD ACCOUNT DATA

When the Payment Gateway (payserv) went live in mid-2010, ScholarChip began storing some sensitive cardholder data. As a result, the following requirements now apply, in order to maintain our compliance with PCI-DSS Requirement 3.1:

- Detailed ScholarChip data storage standards are found in document #31-500, titled ***Data Storage and Encryption Key Management Policy.*** This document must be kept up to date as business needs change, and must detail how and where sensitive cardholder data is allowed to be stored within the organization (i.e. encrypted within database, encrypted within backup media, encrypted within files on disk, within hardcopy documents, etc.). For each storage method and location, the document must define how long data is allowed to be kept (retention period) and contain a justification for its storage.

- ScholarChip data storage standards and procedures must document any legal, regulatory, or business requirements for cardholder data retention.

- All cardholder data older than the stated retention period(s) must be removed from storage locations (online, offline, printed, etc.). All data storage locations must be documented and covered under the data disposal requirements.

3.2 STORAGE AND DISPLAY OF SENSITIVE CREDIT CARD DATA

Detailed ScholarChip data storage standards are found in document #31-500, titled ***Data Storage and Encryption Key Management Policy.*** These standards must comply with the current PCI-DSS Requirements 3.2-3.4, and must always be kept up to date as business needs and regulations change.

NOTE: See the document published by the Payment Card Industry Security Standards Council entitled "PCI-DSS Requirements and Security Assessment Procedures v1.2" p. 4 for definitions of cardholder data types.

3.3 CRYPTOGRAPHIC KEY MANAGEMENT POLICIES

ScholarChip's encryption process and key management policy are outlined in Document #31-500, titled ***Data Storage and Encryption Key Management Policy***. This document must be kept up-to-date in compliance with PCI-DSS Requirements 3.5 and 3.6, and must always include the following:

- Keys used for encryption and decryption of cardholder data must be protected against disclosure and misuse.
- Access to encryption/decryption keys is restricted to only those with a business need to know.
- When storing the data encryption key (DEK), the DEK must be stored encrypted and the key used to encrypt the DEK (the key encryption key or KEK) must be stored separately from the DEK. Store cryptographic keys in the fewest possible locations
- We currently do NOT distribute encryption keys to customers. Should it ever become necessary to change this, customers MUST be given documentation regarding proper key management requirements to meet ScholarChip policies (including PCI-DSS requirements).
- Generate strong cryptographic keys (proper method, strength, and complexity).
- Description of process for secure distribution and storage of all encryption keys utilized for encrypting cardholder data
- Description of process for changing encryption keys annually , replacing keys that are suspected of compromise, and removing/destroying old or invalid keys
- Split knowledge/dual control must be used to reconstruct a data encryption key (i.e.- two or three people, each knowing only their own part of the key, are required to provide input to reconstruct the full data encryption key).
- Controls must be in place that will prevent the unauthorized substitution of encryption keys.
- Encryption key custodians must sign a form signifying they understand and accept their key-custodian responsibilities.

3.4 APPLYING PCI STANDARDS TO OTHER SENSITIVE DATA

Credit card data is not the only sensitive data housed in ScholarChip systems. When applied correctly, PCI standards offer a high level of protection for sensitive data of any kind. Therefore, wherever feasible, PCI-prescribed security controls should be implemented platform-wide, in order to protect

other sensitive classes of data such as personally identifiable information, student education records and behavioral data, etc. However, particular controls may not be feasible for some parts of the platform; they may be too restrictive, too expensive or time-consuming, or simply not warranted. In such cases the risks must be evaluated and documented, and appropriate levels of alternate controls must be selected.

4.0 ENCRYPT TRANSMISSION OF SENSITIVE DATA OVER OPEN, PUBLIC NETWORKS

Sensitive information must be encrypted during transmission over networks that are easily accessed by individuals with malicious intent. Improperly configured wireless networks and vulnerabilities in legacy encryption and authentication protocols can be continued targets of individuals with malicious intent who exploit these vulnerabilities to gain privileged access to sensitive data environments.

4.1 TRANSMISSION OF SENSITIVE DATA OVER PUBLIC NETWORKS

Whenever cardholder data or other sensitive information is transmitted or received over open, public networks, the following criteria must be met to satisfy PCI-DSS Requirement 4.1:

- Strong encryption algorithms and protocols (ex: SSL/TLS*, IPSEC) must be used.
- The latest SSL/TLS* versions must be supported.
- The HTTPS indicator must be part of the URL whenever cardholder data is transmitted or received over open, public networks via a web browser.
- Only SSL certificates* issued by a trusted Certificate Authority are to be used for transmission of cardholder data across open, public networks (inbound or outbound).
- ScholarChip currently does not allow any wireless systems to be used in the card network. However, if this restriction is ever lifted, the use of the WEP protocol will be prohibited. (Requirement effective June 30, 2010.)

*Note – PCI-DSS version 3.2 requires the use of TLS protocol 1.2 instead of SSL, but the certificates are still commonly referred to as SSL certificates.

4.2 TRANSMISSION OF SENSITIVE DATA VIA END USER MESSAGING TECHNOLOGIES

- Transmission of unencrypted cardholder data or other sensitive information via end-user messaging technologies (e.g. e-mail, instant messaging, etc.) is strictly prohibited, as specified by PCI-DSS Requirement 4.2. For specific guidelines, see ***Document 31-026 Information Sensitivity and Privacy Policy***

MAINTAIN A VULNERABILITY MANAGEMENT PROGRAM

System components within the sensitive data environment (cardholder data network) must be part of an active vulnerability maintenance program. This program will control the existence of malicious software (e.g. – anti-virus software) and provide policies covering development efforts and system or software updates/upgrades such that security is maintained. The following policies ensure system components are protected from malicious software and vulnerabilities that result from software bugs and improperly patched applications and operating systems.

5.0 USE REGULARLY UPDATED ANTI-MALWARE SOFTWARE

Malicious software, commonly referred to as "malware"—including viruses, worms, and Trojans—enters a sensitive network segment during many business approved activities, including employees' e-mail and use of the Internet, mobile computers, and storage devices, resulting in the exploitation of system vulnerabilities. Anti-malware (anti-virus) software must be used on all systems commonly affected by malware to protect systems from current and evolving malicious software threats.

5.1 USE ANTI-VIRUS SOFTWARE TO PROTECT SYSTEMS

ScholarChip uses a centrally-managed AntiVirus solution for all servers in the card network. This is in compliance with PCI-DSS Requirements 5.1 and 5.2.

- Anti-virus software MUST be deployed on all systems in the card network that are commonly affected by malicious software. This includes personal computers, servers, etc. that are attached to the cardholder network segment.
- Anti-virus programs MUST be capable of detecting, removing, and protecting against all known types of malicious software (adware, spyware, etc.).
- All anti-virus software and its associated definition files MUST be kept up-to-date at all times.
- All anti-virus software must be actively running, and capable of generating audit logs.
- Anti-virus software audit logs must be retained for one year.

Details of anti-virus setup are outlined in ***Document #31-6060, ScholarChip Antivirus Policy and Configuraton.***

6.0 DEVELOP AND MAINTAIN SECURE SYSTEMS AND APPLICATIONS

Individuals with malicious intent use security vulnerabilities to gain privileged access to systems. Many of these vulnerabilities can be fixed by applying vendor-provided security patches. All critical systems must have the most recently released, appropriate software patches to protect against exploitation and compromise of sensitive data (cardholder data) by individuals with malicious intent and the use of malicious software.

Note: Appropriate software patches are those patches that have been evaluated and tested sufficiently to determine that the patches do not conflict with existing security configurations. For in-house developed applications, the introduction of vulnerabilities can be avoided by using standard system development processes and secure coding techniques.

6.1 REGULARLY UPDATE SYSTEMS AND SOFTWARE

- All system components and software must have the latest vendor-supplied system security patches installed. (PCI-DSS Requirement 6.1).
- All critical system and software patches must be installed within 30 days of vendor release. (PCI-DSS Requirement 6.1).
- Responsibility and schedule for these updates is published in the ***System Configuration Management and Maintenance (SCMM) Policy*** #31-5600.

6.2 STAY INFORMED

ScholarChip technical staff members must:

- Subscribe to outside sources for updated security vulnerability information, in the form of email bulletins or news feeds. For system administrators, these outside sources should include at a minimum:
    - SANS (SysAdmin, Audit, Network, Security) Institute - http://www.sans.org/
    - NIST (National Institute of Standards and Technology) - Computer Security Division – Information Technology Library - http://csrc.nist.gov/
    - Microsoft Security newsletters/bulletins

  Other possible security information sources might includethird party audit firms and security consultants, OWASP, Acunetix, etc.
- Review and update system configuration standards as new vulnerability information might dictate. (PCI-DSS Requirement 6.2).

NOTE: System administrators for card-related systems are specifically named in Appendix A of this policy document. However, developers and other employees who work with sensitive data should also keep up to date on the latest available security information. All employees should consider subscribing to these sources as necessary for their job function.

6.3 SECURE SOFTWARE DEVELOPMENT

Some softwareapplications developed by ScholarChip is used to store, process, or transmit cred card data or other sensitive information. Our development policies and practices must insure that this software is developed and tested in a secure manner.

Detailed software development guidelines can be found in Document #31-600, titled ***ScholarChip Software Development Policy*** and #31-923, ***titled ScholarChip Software Development Methodology Highlights***. All developers must read and understand these guidelines before beginning work on any card-related systems.

6.4 CHANGE CONTROL TRACKING

Change control tracking procedures must capture all changes to system components in the cardholder data network. This includes changes in configuration of firewalls, network hardware, servers, and software used within the cardholder data environment. (PCI-DSS Requirement 6.4) Change control tracking policy is defined in Document #31-3820 and procedures are outlined in detail in Documents #31-4040 for infrastructure changes and #31-3821 for application changes.

All major application change requests must be submitted in writing (either via email or as a "Project" through the management site), and must include the following, in order to comply with PCI-DSS Requirements 6.4.1-6.4.4:

- details on the impact of the change to customers.
- completion of code review
- completion of operational functionality testing, with satisfactory ("passing") results.
- back-out procedures that can be used to return systems to a state before the change was made.
- management sign-off by appropriate parties, at all stages (development, code review, testing, final approval).

ALL OF THESE DETAILS MUST BE PROVIDED and appropriate management sign-offs MUST BE OBTAINED before implementing any major application changes in the production environment.

6.5 WEB APPLICATION DEVELOPMENT

Web applications are particularly vulnerable to internal and external threats which may expose cardholder data and other confidential ScholarChip information. Therefore all web applications must be developed according to strict coding guidelines that minimize this vulnerability.

Detailed software development guidelines can be found in the ***ScholarChip Software Development Policy***, Document #31-600. All developers must read and understand these guidelines before beginning work on any card-related systems.

6.6 PROTECT EXPOSED WEB APPLICATIONS

- Public-facing web applications must be reviewed (using either manual or automated vulnerability security assessment tools or methods) as follows: (PCI-DSS Requirement 6.6)
    a. At least annually
    b. After any changes

c. By an organization that specializes in application security (can be a separate internal company team that has been trained appropriately)
d. All vulnerabilities discovered must be corrected
e. The application must be re-evaluated after corrections have been made

Details on methods used to meet this requirement are outlined in Document #31-923, titled ***Software Development Methodology.***

IMPLEMENT STRONG ACCESS CONTROL MEASURES

Access to system components and software within the sensitive data environment (cardholder data network) must be controlled and restricted to those with a business need for that access. This is achieved through the use of active access control systems, strong controls on user and password management, and restricting physical access to critical or sensitive components and software to individuals with a "need to know".

7.0 RESTRICT DATA ACCESS BY BUSINESS "NEED TO KNOW"

Systems and processes must be in place to limit access to critical data and systems based on an individual's need to know and according to job responsibilities.

"Need to know" is when access rights are granted to the least amount of data and privileges needed to perform a job.

7.1 RESTRICT ACCESS TO CARDHOLDER DATA ENVIRONMENT

- Access to cardholder data and systems handling cardholder data must be restricted by business need to know. (PCI-DSS Requirement 7.1)
- Access to computing resources must be limited to those who have a business need to know and such access must be restricted to the least privileges required to perform job responsibilities. (PCI-DSS Requirement 7.1.1)
- Access privileges will be assigned based on individual personnel's job classification and function. A ***Request for Server Access*** form, Document #31-121, must be generated and signed by management approving the access. (PCI-DSS Requirement 7.1.2 and 7.1.3) Alternatively, email may be used to document access requests, if the email states the reason for the access and shows approval by the system owner or senior technical management .
- Access controls are required on all system components of the cardholder data environment and must be implemented via an automated access control system. (PCI-DSS Requirement 7.1.4)
- Access control systems must be set to a default "deny-all" setting. (PCI-DSS Requirement 7.2)

8.0 ASSIGN A UNIQUE ID TO EACH PERSON WITH ACCESS TO SYSTEM COMPONENTS/SOFTWARE

It is critical to assign a unique identification (ID) to each person with access to critical systems or software. This ensures that each individual is uniquely accountable for his or her actions. When such accountability

is in place, actions taken on critical data and systems are performed by, and can be traced to, known and authorized users.

8.1 REQUIRE UNIQUE USER ID'S

- Unique ID's will be used for all users that access system components in the cardholder data environment. (PCI-DSS Requirement 8.1)

8.2 USER AUTHENTICATION METHODS

- In addition to assigning a unique user ID, access to systems in the card network requires the use of a password, passphrase, or two-factor authentication. (PCI-DSS Requirement 8.2)
- Document all methods of user authentication implemented on each system component within the card network. (PCI-DSS Requirement 8.2)

8.3 TWO-FACTOR AUTHENTICATION

- Two-Factor authentication (authentication that requires you to present something you know and something you have) is required for all non-console administrative access into system components of the cardholder data network. (PCI-DSS Requirement 8.3)

  For further details, see the ***ScholarChip Remote Access Policy***, Document #31-160.

8.4 PROTECT PASSWORDS

- All passwords must be rendered unreadable using strong cryptography during transmission and storage on all system components. (PCI-DSS Requirement 8.4)

8.5 PASSWORD POLICY

- User passwords must be constructed and protected according to the standards outlined in the password section of the ***ScholarChip Access Control Policy***, Document 31-4821. (Formerly a separate document, ***ScholarChip Password Policy,*** Document #31-023.)

9.0 RESTRICT PHYSICAL ACCESS TO SENSITIVE DATA AND CRITICAL SYSTEM COMPONENTS

Any physical access to data or systems that house sensitive data (cardholder data) provides the opportunity for individuals to access devices or data and to remove systems or hardcopies, and should be appropriately restricted.

All of ScholarChip's cardholder network system components are housed in the 6th Avenue Coresite Data Center. This data center meets all physical security criteria specified in PCI-DSS requirements 9.1 – 9.4. For detailed data center specifications, see Document #31-340 and http://www.coresite.com/ourdatacenters-newyork.php. For a list of individuals with authorized access, see ***Document 31-5980, Card Holder Environment Access Control Policy***.

9.1 LIMIT AND MONITOR PHYSICAL ACCESS TO SYSTEMS

- Physical security controls must exist for each computer room, data center, and any other physical areas that contain systems in the cardholder data environment. Use security systems such as badge readers, lock and key, etc. to control access to these areas. (PCI-DSS Requirement 9.1)
- Use video cameras or other access control mechanisms to monitor individual physical access to sensitive areas. Store access data for at least 3 months. (PCI-DSS Requirement 9.1.1)
- Restrict public physical access to network jacks that would provide access to the cardholder data network. (PCI-DSS Requirement 9.1.2)
- Restrict physical access to wireless access points, gateways, network hardware and handheld devices. (PCI-DSS Requirement 9.1.3)

9.2 EMPLOYEE AND VISITOR IDENTIFICATION

All ScholarChip employees have smart cards with a visible photograph. Access to the data center requires a second card and biometric fingerprint access. No visitors are allowed without both a ScholarChip employee escort AND a temporary card.

In order to comply with PCI-DSS Requirement 9.2, ScholarChip must maintain documented HR processes. New hire and termination procedures are outlined in Document #31-741, ***HR Operating Procedures***.

Visitor Log and Badges Storage of cardholder data is restricted to the 6th Avenue data center only. Coresite security staff keeps a written log of visitors to the data center. Visitor badges are only used in the data center, and must be turned in at the end of the visit.

9.3 SECURING BACKUP MEDIA

- Store any media back-ups containing sensitive data in a secure location. Any off-site facility used for storage must be physically reviewed at least annually by a ScholarChip employee. (PCI-DSS Requirement 9.5)

9.4 SECURING HARD COPY MATERIALS

In mid-2010, ScholarChip began storing some sensitive cardholder data. As a result, the following requirements now apply, in order to maintain our compliance with PCI-DSS Requirement 9.6:

Printing hard copies of cardholder data is STRICTLY PROHIBITED. Any paper documents and electronic media containing any other sensitive data must be kept secured.

In order to establish a culture of security and trust for all employees at ScholarChip, we have an informal "Clean Desk Policy". An effective clean desk effort involving the participation and support of all ScholarChip employees can greatly protect paper documents that contain sensitive information. (Additional benefits of a clean desk are increased productivity and a positive professional image when our customers visit the company.)

- At known extended periods away from your desk, such as a lunch break, sensitive working papers are expected to be placed in locked drawers.
- At the end of the working day the employee is expected to tidy their desk and to put away all office papers. ScholarChip provides locking desks and filing cabinets for this purpose.
- If a piece of sensitive documentation is no longer needed, it should be shredded.
- Consider scanning paper items and filing them electronically in a secure location.
- Lock your desk and filing cabinets at the end of the day
- Lock away portable computing devices such as laptops or PDA devices
- Treat mass storage devices such as CDROM, DVD or USB drives as sensitive and secure them in a locked drawer

Use common sense. If in doubt about whether something is considered "sensitive information", err on the side of caution and treat it as such.

For guidelines on protection measures for various types of sensitive data, see the ***ScholarChip Information Sensitivity Policy***, Document #31-026.

9.5 MEDIA TRANSFER AND TRACKING

ScholarChip currently does not store cardholder or other sensitive data on any type of removable media. Should business necessitate storage in the future, the following procedures must be documented and followed, in order to comply with PCI-DSS Requirements 9.7-9.9:

- ScholarChip will define specific procedures required for controlling the internal or external distribution of any kind of media containing cardholder data. Maintain strict control over the storage and accessibility of both hardcopy and electronic media that contains cardholder data. (PCI-DSS Requirement 9.7, 9.9)
- Media must be classified and labeled in such a way that it can be identified as "Confidential". (PCI-DSS Requirement 9.7.1)
- All media containing sensitive cardholder data sent outside the facility must be transferred by secured courier or other delivery method that can be accurately tracked. Log all transfers of media containing cardholder data. Logs must show management approval, and tracking information. Retain media transfer logs. (PCI-DSS Requirement 9.7.2)
- Management approval is required prior to moving any and all media containing cardholder information out of a secured area (especially when media is distributed to individuals). (PCI-DSS Requirement 9.8)
- Periodic inventory of stored media containing cardholder data must be performed and documentation must be retained showing these inventories were performed. (PCI-DSS Requirement 9.9)

9.6 MEDIA DESTRUCTION POLICIES

Very few employees at ScholarChip have direct access to cardholder data, however the following requirements still apply to confidential data at all sensitivity levels. Therefore, when in doubt, don't throw it out – DESTROY IT. More specific guidelines can be found in the ***ScholarChip Information Sensitivity Policy***, Document #31-026.

- Media containing cardholder or other sensitive data must destroyed when it is no longer needed for business or legal reasons. (PCI-DSS Requirement 9.10)
- All paper documents containing potentially sensitive data must be cross-cut or confetti shredded. (PCI-DSS Requirement 9.10.1)
- Whenever a ScholarChip server is decommissioned:
    - the drive must be "zero-wiped" and/or physically destroyed (using a hammer or drill).
    - a log must be kept , recording when and how the drive was wiped/destroyed.

IT IS NOT ENOUGH TO SIMPLY DELETE THE FILES and/or format the disk, as it is sometimes still possible to reconstruct data under these circumstances. (PCI-DSS Requirement 9.10.2)

REGULARLY MONITOR AND TEST SENSITIVE DATA NETWORKS

Important components of overall system security are the regular testing of networks for exposed vulnerabilities and the continuous monitoring of security indicators (logs, system events, etc.). The following policies address system monitoring and vulnerability testing.

10.0 TRACK AND MONITOR ALL ACCESS TO NETWORK RESOURCES AND SENSITIVE DATA

Logging mechanisms and the ability to track user activities are critical in preventing, detecting, or minimizing the impact of a data compromise. The presence of logs in all environments allows thorough tracking, alerting, and analysis when something does go wrong. Determining the cause of a compromise is very difficult without system activity logs.

10.1 MONITOR SYSTEM COMPONENTS WITHIN THE CARDHOLDER DATA NETWORK

- ScholarChip has enabled audit trails (active system tracking logs) on all system components within the cardholder data network (e.g. – server event logs, web server logs, firewall logs, payment application logs, etc.). (PCI-DSS Requirement 10.1)
- Only individuals who have a job-related need will have access to audit trail files. For details, see ***Doc #31-740 Log Monitoring Process*** Notes , and also Appendix A of this policy document(PCI-DSS Requirement 10.5)
- All audit trail logs (e.g. – System logs, IDS logs, firewall logs, web logs, etc.) will be reviewed daily, as described in the ***Log Monitoring Process Notes***, Document #31-740. Noted exceptions must be followed-up on. (PCI-DSS Requirement 10.6)
- All audit trail logs must be retained for 12 months. The most recent three months' logs must be available for immediate review. (PCI-DSS Requirement 10.7)

10.2 NETWORK AND SYSTEM TIME SYNC

ScholarChip is required to define and document the process for obtaining and distributing a time signal (system time) to all system components within the cardholder data network. In order to comply with PCI-DSS Requirement 10.4, the process must meet the following criteria:

- Only known stable versions of NTP (or similar technology) may be used for time servers. These must be regularly updated.
- Time synchronization methodology must only allow a time signal input from known authorized external time sources. Only a designated few (two or three) internal time servers are allowed to

receive external time signals and all other internal devices must synchronize their system time with these internal time servers.

- Internal ScholarChip documentation must identify each internal time server and the specific external time sources from which those servers are allowed to receive a time signal.

  See Document #31-360, titled ***Time Synchronization***, for the acceptable time synchronization methodology to be used for all ScholarChip system components.

11.0 REGULARLY TEST SECURITY SYSTEMS AND PROCESSES

Vulnerabilities are being discovered continually by malicious individuals and researchers, and being introduced by new software. System components, processes, and custom software must be tested frequently to ensure security controls continue to reflect a changing environment.

This policy defines the minimum testing requirements that satisfy PCI-DSS Requirement 11; however, system administrators should keep up-to-date on new security threats and run additional testing as necessary.

For details on all testing procedures, including scheduling and approved tools and vendors, see ***ScholarChip Security and Compliance Planning Procedures*** Document #31-4000.

11.1 ROGUE WIRELESS NETWORK DETECTION

- A wireless analyzer must be used at least quarterly to detect unauthorized wireless networks/devices within the card-processing environment. (PCI-DSS Requirement 11.1) For detection methods, see ***Doc #31-5981***.

11.2 VULNERABILITY ASSESSMENT SCANS

Regular internal and external vulnerability scans must be performed in order to identify weaknesses that might allow outsiders to gain access to our systems and sensitive data. These scans must be performed according to the following guidelines in order to satisfy PCI-DSS Requirement 11.2:

- Internal vulnerability assessment scans must be performed at least quarterly and after any significant change in the cardholder data network (e.g. changes in firewall rules, or upgrades to products within the environment, etc.).

- External vulnerability scans are to be performed at least quarterly and after any significant change in the cardholder data network (e.g. changes in firewall rules, or upgrades to products within the environment, etc.). All scans must be conducted by an Approved Scanning Vendor (ASV). Scans must be run on all external IP addresses that could be used to gain access to the cardholder data environment.

- Systems failing a vulnerability assessment scan (either internal or external) are to be remediated and retested until a passing scan is achieved.
- Results of each quarter's internal and external vulnerability assessments are to be documented and retained for review.

11.3 PENETRATION TESTING

Network penetration testing involves hiring someone to try to "break in" to our systems, to see if it can be done easily. This test must be performed according to the following guidelines in order to satisfy PCI-DSS Requirement 11.3:

- External penetration tests are to be performed at least annually and after any significant change in the cardholder data network (e.g. changes in firewall rules, or upgrades to products within the environment, etc.). All external IP addresses that could be used to gain access to the cardholder data environment must be tested.
- Segmentation testing is to be performed every 6 months and after significant changes to segmentation controls.
- Penetration testing is to be performed by a qualified internal resource or external third party. The asset conducting the penetration test must be independent from personnel that work within the cardholder environment.
- Penetration tests must include both a network-layer and application-layer testing.
- Results of penetration tests must be documented and retained for review.
- For penetration test methodology used by ScholarChip, see ***Doc #31-6080 Penetration Test Scope*** and ***#31-6081 Penetration Test Rules of Engagement***.

11.4 INTRUSION DETECTION/PREVENTION

- All traffic within the cardholder data environment must be monitored by the use of an Intrusion Detection System (IDS) and/or Intrusion Prevention System (IPS). (PCI-DSS Requirement 11.4)
- All IDS/IPS system(s) must be kept up-to-date with the latest available attack signatures. (PCI-DSS Requirement 11.4)
- File Integrity Monitoring software must be deployed on all systems within the cardholder data environment and be configured to monitor all critical files, including system files, application files, log files, stored encryption keys, etc. (PCI-DSS Requirement 11.5)

MAINTAIN AN INFORMATION SECURITY POLICY

A strong security policy sets the security tone for ScholarChip and informs employees and vendors what is expected of them.

In order for this Security Policy to fulfill its purpose, it must be distributed, reviewed, updated and most importantly, FOLLOWED. All employees and vendors should be aware of the sensitivity of data and their responsibilities for protecting it. Not only is this common sense, but it is also explicitly stated in PCI-DSS Requirement 12 and its sub-requirements. Therefore, ScholarChip must have a formal security awareness program to inform all employees of their security responsibilities. This section will address the various components of the security awareness program.

Without consistent application of strong security policies and procedures, even the strictest security controls cannot do their job. They break down due to inattention and poor maintenance, and thus become ineffective at preventing data breech. The following documentation policies address maintaining the ScholarChip security policies described above.

12.0 SECURITY PROCEDURES FOR EMPLOYEES AND CONTRACTORS

12.1 DISTRIBUTE AND UPDATE POLICY AND PROCEDURES

- ScholarChip requires that the most recent version of the information security policy be published and disseminated to all relevant system users (including vendors, contractors, and business partners).

- ScholarChip will follow a risk assessment process that evaluates systems and processes within the cardholder data network and focuses on identifying threats, vulnerabilities, and results in a formal risk assessment. This process is outlined in the document titled ***ScholarChip Risk Assessment Process***, Document #31-660. (PCI-DSS Requirement 12.1)

- The ***ScholarChip Information Security Policy*** must be reviewed at least annually to keep it up to date with changes in the industry and with any changes in the cardholder network environment. (PCI-DSS Requirement 12.1.3)

- Regularly-scheduled operational security and maintenance procedures must be documented and followed. These procedures must be consistent with the PCI-DSS, must include administrative and technical procedures for each of the applicable requirements, and must be kept up to date as system requirements change. (PCI-DSS Requirement 12.2)

  Current operational procedures can be found in Document #31-4000 ***Security and Compliance Planning Procedures (SCPP).***

12.2 EMPLOYEE FACING TECHNOLOGIES

- ScholarChip employees must follow documented usage policies for all critical "employee-facing technologies" (e.g. remote-access technologies, wireless technologies, removable electronic media, laptops, personal data/digital assistants (PDAs), e-mail usage and Internet usage). For details, see ***ScholarChip Acceptable Use Policy***, Document #31-024. (PCI-DSS Requirement 12.3)

12.3 ASSIGN INFORMATION SECURITY RESPONSIBILITIES & TRAIN EMPLOYEES

In order to remain PCI-DSS compliant, ScholarChip must have documented formal information security procedures, including assignment of specific roles/responsibilities and an ongoing security training/awareness program.

Assignment of Responsibilities - ScholarChip's information security policy and procedures must clearly define the information security responsibilities of both employees and contractors. (PCI-DSS Requirement 12.4)

Responsibilities of information security at ScholarChip must be formally assigned to a specific individual(s), position, or team. (PCI-DSS Requirement 12.5)

At a minimum, the following responsibilities must be assigned:

- Creation and distribution of ScholarChip information security policies and procedures
- Responsibility to monitor, analyze, and distribute security alerts and information.
- Creation and distribution of security incident response and escalation procedures
- Responsibility to administer users in the cardholder data network. Includes all additions, deletions and modifications to user access.
- Responsibility to monitor and control all access to sensitive cardholder data.

For current security responsibility assignments, see Appendix A of this document.

Training/Awareness - (PCI-DSS Requirement 12.6.1) Employees working with sensitive data must be educated upon hire and at least annually regarding their data security responsibilities. Security awareness training programs must employ the use of multiple methods of communicating awareness and educating employees. (e.g. - posters, letters, memos, web, meetings, etc.).

ScholarChip will educate employees via the program outlined in Document #31-1781, ***Security Awareness and Compliance Training***. Participation in this program is required for all employees and contractors working within the cardholder data environment. Additional methods may be used to communicate new security information as deemed necessary.

All employees must acknowledge in writing at least annually that they have read and understood the ScholarChip security policies and procedures. Policy updates will be distributed by the Compliance Officer after every review cycle on an as-needed basis. Each new version must be read thoroughly and acknowledged by signing and returning the form on the last page.

12.4 BACKGROUND CHECKS

- Background checks must be conducted prior to hire (within the constraints of local laws) on new employees who will have access to sensitive data or the cardholder data environment. (PCI-DSS Requirement 12.7) Additional periodic screening may be required based on job function and client requests. Details are outlined in Doc 31-741, ***HR Operating Procedures***.

12.5 POLICIES FOR SHARING SENSITIVE DATA WITH SERVICE PROVIDERS

If sensitive data is shared with service providers (for example, back-up tape storage facilities, managed service providers such as Web hosting companies or security service providers, or those that receive data for fraud modeling purposes), the following policies and procedures must be followed:

- Sharing of data must be authorized by system owner, technical management and/or Compliance department.
- ScholarChip must maintain a documented list of any service provider that is given sensitive data, provided direct access to the cardholder network, or can affect the security of the cardholder network. (PCI-DSS Requirement 12.8.1)
- Any written agreement with a service provider that is given sensitive data, provided direct access to the cardholder network, or can affect the security of the cardholder network, must include an acknowledgement of the service provider's responsibility for securing all sensitive data they receive from ScholarChip. (PCI-DSS Requirement 12.8.2)
- Prior to engaging with a service provider that is given sensitive data, provided direct access to the cardholder network, or can affect the security of the cardholder network, ScholarChip will conduct due diligence and follow an established process to ensure that the security of sensitive data within the service providers network has been addressed. (PCI-DSS Requirement 12.8.3) See ***Document 31-5880 Vendor Management Procedures***.
- ScholarChip will have an ongoing program to monitor the PCI DSS compliance status of any service provider that is given sensitive data, provided direct access to the cardholder network, or can affect the security of the cardholder network. (PCI-DSS Requirement 12.8.4)

12.6 INCIDENT RESPONSE PLAN POLICY

Incidents or suspected incidents regarding the security of the cardholder data network or cardholder data itself must be handled quickly and in a controlled, coordinated and specific manner. An incident response plan must be developed and followed in the event of a breach or suspected breach. The current ***ScholarChip Incident Response Plan*** can be found on the document management site, Document #31-300. The general process for responding to an incident is illustrated in the ***Incident Response Flowchart***, Document #31-420.

The plan must meet the following criteria, in order to comply with PCI-DSS Requirement 12.10 and all its sub-requirements:

- The IRP must clearly define roles & responsibilities for response team members.
- The IRP must define communication strategies to be used in the event of a compromise including notification of payment brands.
- The IRP must define specific incident response procedures to be followed.
- The IRP must document business recovery and continuity procedures.
- The IRP must detail all data back-up processes.
- The IRP must contain an analysis of all legal requirements for reporting compromises of sensitive data (for example, California Bill 1386 which requires notification of affected consumers in the event of an actual or suspected compromise of California residents data).
- The IRP must address coverage and responses for all critical system components.
- The IRP must include or reference the specific incident response procedures from the payment brands.
- The IRP must be tested at least annually (maintain evidence that can be validated showing that testing is being performed as per policy).
- ScholarChip must designate specific personnel to be available on a 24/7 basis to respond to alerts. This 24/7 coverage needs to include incident response and monitoring coverage for any evidence of unauthorized activity, detection of unauthorized wireless access points, critical IDS alerts, and reports of unauthorized critical system or application file changes.
- Require that staff with security breach responsibilities (as defined in the IRP) is periodically trained on their response procedures.
- A detailed process and/or procedure for monitoring critical security breach indicators (event logs, IDS logs, File Integrity report, wireless scans or wireless IDS logs etc.) must be defined and documented in the IRP.
- A process must be in place for modifying and evolving the IRP according to lessons learned and integrating best practices as the industry develops, and whenever changes are made to any component in the cardholder network. (PCI-DSS Requirement 12.9.6)

APPENDIX A – SECURITY ROLES AND RESPONSIBILITIES

As mentioned in section 12.3 of this policy, the following are the assigned roles for security processes as of 2018:

Name of Individual or Group	Description of Responsibility
Maged Atiya	CEO/CTO - Overall responsibility for Information Security strategies and implementation Establish · system configuration standards · incident response and escalation policies
	Incident Response Team (must be available 24/7). Ultimate responsibility lies with CTO. Other team leaders include Seth Schultz, Tim Mui
Maged Atiya, Craig Lockwood, Donna Harrigan	Annual risk assessment process
Donna Harrigan	Establish, document and distribute security policies Establish, document and distribute privacy policies and practices Document and distribute · system configuration standards · incident response and escalation policies Establish/oversee security awareness/training program; track employee participation
Kathy Ecoffey Donna Harrigan	Employee onboarding/offboarding processes related to security Screen potential employees prior to hire and rescreen periodically as needed
Tim Mui Alshane McDonald	Security Operations - Monitor, test and maintain overall network infrastructure Monitor, analyze, and distribute security alerts and information; Review security logs and follow up on exceptions

Seth Schultz Tim Mui	Administration of user accounts on systems in the cardholder data network; Monitor and control all access to cardholder data Ensure that all system components and software have the latest security patches installed
Seth Schultz	Implement Secure Software Development Lifecycle for applications in the cardholder environment
Seth Schultz, Managers	Approve/sign · system access requests · change control documentation

APPENDIX B – AGREEMENT TO COMPLY

Agreement form on the next page must be signed by employee upon hire and kept on file in HR.

AGREEMENT TO COMPLY WITH INFORMATION SECURITY POLICIES

A signed paper copy of this form must be submitted by all employees working with sensitive cardholder data. ScholarChip management will not accept modifications to the terms and conditions of this agreement.

Employee Name (Print)	
Department/Title	
Phone Number	

I, the user, agree to take all reasonable precautions to assure that ScholarChip internal information, or information that has been entrusted to ScholarChip by third parties such as customers, will not be disclosed to unauthorized persons. At the end of my employment or contract with ScholarChip, I agree to return to ScholarChip all information to which I have had access as a result of my position with ScholarChip. I understand that I am not authorized to use this information for my own purposes, nor am I at liberty to provide this information to third parties without the express written consent of the internal ScholarChip manager who is the designated information Owner.

I have access to a copy of the ScholarChip Information Security Policies Manual, I have read and understand the manual, and I understand how it impacts my job. As a condition of continued employment at ScholarChip, I agree to abide by the policies and other requirements found in that manual. I understand that non-compliance will be cause for disciplinary action up to and including system privilege revocation, dismissal from ScholarChip, and perhaps criminal and/or civil penalties.

I agree to choose a difficult-to-guess password as described in the ScholarChip Information Security Policies Manual, I agree not to share this password with any other person, and I agree not to write this password down unless it has been transformed in an unrecognizable way.

I also agree to promptly report all violations or suspected violations of information security policies to the Chief Security Officer.

_____ _____

Employee's Signature Date