Services Agreement with the Phoenix Central School District

This Agreement, made this October 1, 2021 ("Effective Date"), by and between the Phoenix Central School District ("School District"), having an office at 116 Volney Street, Phoenix, NY 13135 and , Keeper Security, Inc. ("Vendor") having an office at 820 W. Jackson Blvd., Suite 400, Chicago, IL 60607 (collectively the "Parties").

In consideration of the mutual promises and covenants contained herein, the Parties agree as follows:

1.

Services. Vendor shall perform the services set forth in this Agreement, as described in Addendum C (the "Services"). Vendor shall provide the Services at the School District location or on a remote basis, as agreed to by the Parties. Vendor warrants that the Services provided hereunder will be performed in a good and workmanlike manner.

License. Vendor hereby grants to School District, including to all School District's authorized users, a non-exclusive, non-sublicensable, non-assignable and royalty-free license to access and use the service (the "Services") solely for School District's operations in accordance with the terms of this Agreement.

Services. Vendor hereby grants to School District, including to all School District's authorized users, a non-exclusive, non-sublicensable, non-assignable and royalty-free license to access and use the service(s) and/or program(s). The Vendor shall further perform related services and any additional services as set forth in Addendum C (collectively, "Services"). Vendor shall provide the Services at the School District location or on a remote basis, as agreed to by the Parties. Vendor warrants that the Services provided hereunder will be performed in a good and workmanlike manner.

2. **Term of Services**. This Agreement begins on the Effective Date and will continue unless terminated earlier as set forth herein (the "Term").

3. **Termination.** This Agreement may be terminated as follows:

(a) By the School District immediately in the event of breach by the Vendor;

(b) By either Party in the event of a Default not cured within the time period set forth in Section 7 herein; and

4. **Payment**. Payment shall be made in accordance with Addendum D attached hereto.

5. **Protection of Confidential Data**. Vendor shall provide its Services in a manner which protects Student Data (as defined by 8 NYCRR 121.1(q)) and Teacher or Principal Data (as defined by 8 NYCRR 121.1(r)) (hereinafter "Confidential Data") in accordance with the requirements articulated under Federal, State and local laws and regulations, including but not limited to the foregoing:

(a) Vendor will adopt technologies, safeguards and practices that align with the NIST Cybersecurity Framework.

(b) Vendor will comply with the School District Data Security and Privacy Policy, Education Law § 2-d, and 8 NYCRR §121.

(c) Vendor will limit internal access to personally identifiable information to only those employees or sub-contractors that need access to provide the contracted services.

(d) Vendor will not use the personally identifiable information for any purpose not explicitly authorized in this Agreement.

(e) Vendor will not disclose any personally identifiable information to any other party without the prior written consent of the parent or eligible student, unless otherwise authorized pursuant to applicable law.

(f) Vendor will maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of personally identifiable information in its custody.

(g) Vendor will use encryption to protect personally identifiable information in its custody while in motion or at rest.

(h) Vendor will not sell personally identifiable information nor use or disclose it for any marketing or commercial purpose or facilitate its use or disclosure by any other party for any marketing or commercial purpose or permit another party to do so.

(i) In the event Vendor engages a subcontractor to perform its contractual obligations, the data protection obligations imposed on the Vendor shall apply to the subcontractor.

6. **Data Breach**. In the event that Confidential Data is accessed or obtained by an unauthorized individual, Vendor shall provide notification to the School District without unreasonable delay and not more than seven calendar days after the discovery of such breach. Vendor shall follow the following process:

(a) The security breach notification shall be titled "Notice of Data Breach," shall be clear, concise, use language that is plain and easy to understand, and to the extent available, shall include: a brief description of the breach or unauthorized release; the dates of the incident and the date of discovery;

a description of the types of Confidential affected; an estimate of the number of records affected; a brief description of the vendors investigation or plan to investigate; and contact information for representatives who can assist the School District with additional questions.

(b) The Vendor shall also prepare a statement for parents and eligible students which provides information under the following categories: "What Happened," "What Information Was Involved," "What We Are Doing," "What You Can Do," and "For More Information."

(c) Where a breach or unauthorized release of Confidential Data is attributed to Vendor, and/or a subcontractor or affiliate of Vendor, Vendor shall pay for or promptly reimburse the School District for the cost of notification to parents and eligible students of the breach.

(d) Vendor shall cooperate with the School District and law enforcement to protect the integrity of investigations into the breach or unauthorized release of Confidential Data.

(e) Vendor further acknowledges and agrees to have a written incident response plan that is consistent with industry standards and federal and state law for responding to a data breach, breach of security, privacy incident or unauthorized acquisition or use of Protected Data or any portion thereof. Upon request, Vendor shall provide a copy of said written incident response plan to the School District.

7. Indemnification. Vendor shall at all times (both during and after the Term of this Agreement), indemnify, defend and hold harmless the School District, its agents, employees and students (collectively for purposes of this Section "the School District"), from and against any and all settlements, losses, damages, costs, counsel fees and all other expenses relating to or arising from (a) Vendor's failure to comply with the terms of this Agreement; and/or (b) the negligent operations, acts or omissions of the Vendor.

8. Assignment. This Agreement is binding upon the Parties and their respective successors and assigns, but Vendor's obligations under this Agreement are not assignable without the prior written consent of the School District. Any assignment without the School District's consent shall be null and void.

9. Default. The School District shall be in Default under this Agreement if the School District fails to pay any fees or charges or any other payments required under this Agreement when due and payable, and such failure continues for a period of fifteen (15) days after receipt written notification of such failure. The Vendor shall be in default of this Agreement if it becomes insolvent, dissolves, or assigns its assets for the benefit of its creditors, or files or has filed against it any bankruptcy or reorganization proceeding.

10. Intellectual Property. Intellectual property rights arising from the Services (but not the data, materials or content provided by Client) shall remain the property of Vendor, and nothing contained in any work product shall be construed to transfer, convey, restrict, impair or deprive Vendor of any of its ownership or proprietary interest or rights in technology, information or products that existed prior to the provision of deliverables under this Agreement or that may be independently developed by Vendor outside the scope of the services provided under this Agreement and without use of any confidential or otherwise restricted material or information thereunder.

11. Governing Law. This Agreement and any Services procured hereunder shall be governed by the laws of the State of New York both as to interpretation and performance, without regard to its choice of law requirements. Each party consents and submits, for any dispute arising out of or relating to this Agreement or the transactions contemplated hereby, to the sole and exclusive jurisdiction of the state and federal courts located in the county in which the School District is located.

12. Compliance with Laws. Vendor, its employees and representatives shall at all times comply with all applicable Federal, State and local laws, rules and regulations.

13. Independent Relationship. It is expressly intended by the Parties hereto, and Vendor hereby specifically warrants, represents and agrees, that Vendor and the School District are independent entities. The Parties intend that this Agreement is strictly between two independent entities and does not create an employer/employee relationship for any purpose. Vendor shall perform the duties contemplated by this Agreement as an independent entity, to whom no benefits shall accrue except for those benefits expressly set forth in this Agreement.

14. Public Inspection of Agreement. Vendor acknowledges and agrees that this Agreement and all documents Vendor provides to School District as required herein, are public records and may at all times be subject to public inspection.

15. Waiver. No delay or omission of the School District to exercise any right hereunder shall be construed as a waiver of any such right and the School District reserves the right to exercise any such right from time to time, as often as may be deemed expedient.

16. Addendums. The following Addendums are attached hereto and incorporated herein:

- Addendum A: Parents' Bill of Rights for Data Privacy and Security
- Addendum B: Parents' Bill of Rights – Supplemental Information Addendum
- Addendum C: Product Specifications and Pricing Table
- Addendum D: Technical Specifications (Omitted)
- Addendum E: Vendor's Data Security and Privacy Plan
- Addendum F: Schedule of Data
- Addendum G: Joinder Agreement

17. Severability. Should any part of this Agreement for any reason be declared by any court of competent jurisdiction to be invalid, such decision shall not affect the validity of any remaining portion, which remaining portion shall continue in full force and effect as if this Agreement had been executed with the invalid portion hereof eliminated, it being the intention of the Parties that they would have executed the remaining portion of this Agreement without including any such part, parts or portions which may for any reason be hereafter declared invalid.

18. Entire Agreement. This Agreement and its attachment constitute the entire Agreement between the Parties with respect to the subject matter hereof and shall supersede all previous negotiations, commitments and writings. It shall not be released, discharged, changed or modified except by an instrument in writing signed by a duly authorized representative of each of the Parties.

IN WITNESS WHEREOF, the partied have executed this Agreement intending to be legally bound.

Phoenix Central School District

Signature

Christopher J. Byrne

Printed Name

Superintendent

Title

Keeper Security, Inc.

DocuSigned by:
Nikki Jamison
E785D1780103443C...

Signature

Nikki Jamison

Printed Name

Associate Corporate Counsel

Title

Addendum A

PHOENIX CSD PARENTS' BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY

Parents (includes legal guardians or persons in parental relationships) and Eligible Students (student 18 years and older) can expect the following:

1. A student's personally identifiable information (PII) cannot be sold or released for any commercial purpose. PII, as defined by Education Law § 2-d and FERPA, includes direct identifiers such as a student's name or identification number, parent's name, or address; and indirect identifiers such as a student's date of birth, which when linked to or combined with other information can be used to distinguish or trace a student's identity. Please see FERPA's regulations at 34 CFR 99.3 for a more complete definition.

2. The right to inspect and review the complete contents of the student's education record stored or maintained by an educational agency. This right may not apply to parents of an Eligible Student.

3. State and federal laws such as Education Law § 2-d; the Commissioner of Education's Regulations at 8 NYCRR Part 121, the Family Educational Rights and Privacy Act ("FERPA") at 12 U.S.C. 1232g (34 CFR Part 99); Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. 6501-6502 (16 CFR Part 312); Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h (34 CFR Part 98); the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. 1400 et seq. (34 CFR Part 300); protect the confidentiality of a student's identifiable information.

4. Safeguards associated with industry standards and best practices including but not limited to encryption, firewalls and password protection must be in place when student PII is stored or transferred.

5. A complete list of all student data elements collected by NYSED is available at

http://www.nysed.gov/data-privacy-security/student-data-inventory and by writing to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234.

6. The right to have complaints about possible breaches and unauthorized disclosures of PII addressed. Complaints may be submitted to NYSED at http://www.nysed.gov/data-privacy-security/report-improper-disclosure , by mail to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234; by email to privacy@nysed.gov; or by telephone at 518-474- 0937. Complaints regarding student data breaches can also be directed to: Michael Foley, Director Data and Instructional Technology, Phoenix Central School District, 116 Volney Street, Phoenix NY, 13135. Phone: 315-695-1549 email: mfoley@phoenixcsd.org.

7. To be notified in accordance with applicable laws and regulations if a breach or unauthorized release of PII

occurs.

8. Educational agency workers that handle PII will receive training on applicable state and federal laws, policies, and safeguards associated with industry standards and best practices that protect PII.

9. Educational agency contracts with vendors that receive PII will address statutory and regulatory data privacy and security requirements.

Addendum B

PARENTS' BILL OF RIGHTS – SUPPLEMENTAL INFORMATION ADDENDUM

1. As used in this Addendum B, the following terms will have the following meanings:

a. "Student" shall have the meaning defined in Subsection 1(f) of Section 2-d.

b. "Eligible Student" shall have the meaning defined in Subsection 1(g) of Section 2-d.

c. "Personally Identifiable Information" as applied to Student Data shall have the meaning defined in Subsection 1(d) of Section 2-d.

d. "Student Data" means Personally Identifiable Information from student records that Vendor receives from the Phoenix Central School District.

Other capitalized terms used in this Addendum B will have the applicable meaning set forth elsewhere in this Agreement or in Section 2-d.

2. Vendor agrees that the confidentiality of Student Data shall be maintained in accordance with state and federal laws that protect the confidentiality of Student Data.

3. Vendor agrees that any of its officers or employees, and any officers or employees of any assignee of Vendor, who have access to Student Data will be provided training on the federal and state law governing confidentiality of such Student Data prior to receiving access to that data.

4. The exclusive purpose for which Vendor is being provided access to Student Data is to permit Vendor to provide Services as set forth in the Agreement. Student Data received by Vendor, or by any assignee of Vendor or third party contracting with Vendor, shall not be sold or used for marketing purposes.

5. If Vendor comes into possession of Student Data, Vendor will only share such Student Data with additional third parties if those third parties are contractually bound to adhere to data protection and security requirements, including but not limited to those outlined in applicable state and federal laws and regulations (e.g., Family Educational Rights and Privacy Act ("FERPA"); Education Law §2-d; 8 NYCRR Part 121).

6. The Contract commences and expires on the dates set forth in the Contract, unless earlier terminated or renewed pursuant to the terms of the Contract. On or before the date the Contract expires, protected data will be exported to the Phoenix Central School District in excel, or other format agreed upon by both Parties. format and/or destroyed by the Contractor as directed by the Phoenix Central School District.

7. If a parent, Student, or Eligible Student wishes to challenge the accuracy of any "education record", as that term is defined in the FERPA, by following the School District's procedure for requesting the amendment of education records under the FERPA. Teachers and principals may be able to challenge the accuracy of APPR data stored by the Phoenix Central School District in Contractor's product and/or service by following the appeal procedure in the School District's APPR Plan. Unless otherwise required above or by other applicable law, challenges to the accuracy of the Confidential Data shall not be permitted.

8. Student Data transferred to Vendor by the Phoenix Central School District will be stored in electronic memory (on servers or other computers) operated and maintained by or on behalf of Vendor in the United States. The measures that Vendor will take to protect the privacy and security of Student Data while it is stored in that manner include, but are not necessarily limited to: encryption to the extent required by Section 2-d; restricted physical access to the servers/computers; software-based solutions intended to prohibit unauthorized entry such as regularly updated virus scans, firewalls, and use of passwords; and administrative controls such as selective user access rights. The measures that Vendor takes to protect Confidential Data will align with the NIST Cybersecurity Framework.

9. The Contractor will apply encryption to the Confidential Data while in motion and at rest at least to the extent required by Education Law Section 2-d and other applicable law.

Addendum C

PRODUCT SPECIFICATIONS AND PRICING TABLE

Keeper Security, Inc.
820 W. Jackson Blvd., Suite 400
Chicago, IL 60607
(312) 829-2680
www.keepersecurity.com

Quote Number	820421
Created Date	9/10/2021
Expiration Date	10/10/2021
Subscription Term (Yrs)	1.00

Customer Information:

Account Name	phoenixcsd.org
Contact Name	Michael Foley
Bill To	116 Volney St. Phoenix, NY 13135 United States
Email	mfoley@phoenixcsd.org

Prepared By	Josh Rhees
Email	jrhees@keepersecurity.com

Product Code	Product	Product Description	Sales Price	Quantity	Discount	Total Price
KS-STORAGE_100_GB	Keeper - 100 GB Storage	Keeper - 100 GB Storage	USD 125.00	1.00	40.00%	USD 75.00
KS-AUDIT	Keeper - Advanced Reporting & Alerts Module	Prevent, detect and isolate security threats.	USD 10.00	10.00	40.00%	USD 60.00
KS-BREACHWATCH	Keeper - BreachWatch for Business	BreachWatch for Business	USD 20.00	10.00	40.00%	USD 120.00
KEEPER-SECURITY-ENT	Keeper - Enterprise Base Plan User Licenses	Term-based subscription for access to Keeper on unlimited devices.	USD 60.00	10.00	40.00%	USD 360.00

Subtotal	USD 1,025.00
Discount	40.00%
Grand Total	USD 615.00

Addendum D

TECHNICAL SPECIFICATIONS
Omitted

Addendum E

VENDOR'S DATA SECURITY AND PRIVACY PLAN

Keeper Security, Inc.'s Privacy Policy is located at https://keepersecurity.com/en_GB/privacypolicy.html. By using our Software, you accept and agree to all terms, provisions and conditions of the Privacy Policy. Keeper Security reserves the right to change the Privacy Policy and will notify you of such changes via email or our website. If we make any material changes we will notify you by email or notification on the keepersecurity.com website prior to the change becoming effective. If you have questions or concerns regarding the Privacy Policy, you may contact us at security@keepersecurity.com

Keeper Security, Inc.

Information Security Policy

I. POLICY

A. General Policy
It is the policy of Keeper Security Inc. that information, as defined hereinafter, in all its forms--written, spoken, recorded electronically or printed--will be protected from accidental or intentional unauthorized modification, destruction or disclosure throughout its life cycle. This protection includes an appropriate level of security over the equipment and software used to process, store, and transmit that information.

B. Documentation, Change, and Approval
All policies and procedures must be documented and made available to individuals responsible for their implementation and compliance. All activities identified by the policies and procedures must also be documented. All the documentation, which may be in electronic form, must be retained after initial creation, or, pertaining to policies and procedures, after changes are made. All documentation must be periodically reviewed for appropriateness and currency, a period of time to be determined by each entity within Keeper Security Inc. Changes to policies and procedures must be approved by senior executive management. Policies and procedures must be reviewed for compliance with legal and contractual obligations, and approved on an annual basis by senior executive management (CEO and CTO).

C. Department Policy
At each entity and/or department level, additional policies, standards and procedures will be developed detailing the implementation of this policy and set of standards, and addressing any additional information system functionality in such entity and/or department. All departmental policies must be consistent with this policy. All systems implemented after the effective date of these policies are expected to comply with the provisions of this policy where possible. Existing systems are expected to be brought into compliance where possible and as soon as practical.

II. SCOPE

A. Scope of Information Security Policy
The scope of information security includes the acceptable use of electronic resources, risk management, protection of the confidentiality, integrity and availability of information.

B. Applicability of Information Security Policy
The framework for managing information security in this policy applies to all Keeper Security Inc. entities and workers, and other Involved Persons and all Involved Systems throughout Keeper Security Inc. as defined below in INFORMATION SECURITY DEFINITIONS.

C. Definitions

This policy and all standards apply to all classes of protected information in any form as defined in the DATA CLASSIFICATION POLICY.

D. Additional Related Policies

In addition to this INFORMATION SECURITY POLICY, the additional security policies and plans must be maintained:

- Acceptable Use Policy
- Data Classification Policy
- Access Control Policy
- Password Policy
- Personal Device Policy
- Disaster Recovery Plan
- Incident Response Plan
- Business Continuity Plan
- Supplier Security Policy
- Secure Systems Engineering Policy
- Legal, Regulatory, and Contractual Requirements Policy
- Operating Procedures for IT Management

Executive Management or the Information Security Officer may develop additional security policies as is necessary to ensure legal or regulatory compliance or to ensure the security of Keeper Security Inc systems, people, and resources.

III. RISK MANAGEMENT

A. Threat Detection and System Analysis

Threat detection and system monitoring is a daily, ongoing activity at the company. An analysis of all Keeper Security Inc. information networks and systems will be conducted every six months to document any threats and vulnerabilities to stored and transmitted information. The analysis will examine the types of threats – internal or external, natural or manmade, electronic and non-electronic -- that affect the ability to manage the information resource. The analysis will also document the existing vulnerabilities within each entity which potentially expose the information resource to the threats. Finally, the analysis will also include an evaluation of the information assets and the technology associated with its collection, storage, dissemination and protection.

B. Frequency of Risk Assessment and Business Impact Analysis

From the combination of threats, vulnerabilities, and asset values, an estimate of the risks to the confidentiality, integrity and availability of the information will be determined. The frequency of the risk analysis will occur as determined necessary by the ISO or Senior Management, or not less than once per calendar year. This Risk Assessment and Business Impact Analysis shall be updated annually and tracked in JIRA or Confluence.

C. Threat Mitigation

Based on the periodic assessment, measures will be implemented that reduce the impact of the threats by reducing the amount and scope of the vulnerabilities.

D. Technology Status Meeting

A Technology Status Meeting shall be held at least once per month to discuss technology issues, environmental, regulatory, security concerns, potential problems, risks, patches and/or security updates, current project status, and potential improvements that could affect the company's ability to meet service level agreements. Meetings shall normally take place no less than once per calendar month, or more frequently as-needed. Issues that require action shall be tracked with a JIRA request in the appropriate project queue.

E. Vulnerability/Penetration Testing

Production systems shall be tested daily by a third-party testing service. Alerts and Findings shall be delivered directly to the CTO, Information Security Officer, and Security Administrators. All discovered vulnerabilities must be fixed or mitigated. The timeline to fix a discovered a vulnerability is determined by the severity of the vulnerability and will be determined by the ISO. On a monthly basis, a meeting shall be held to track review of

the penetration/vulnerability reports by Systems Management and ISO. Any resulting actions from the formal review shall be opened as issues and tracked in JIRA.

F. Firewall Auditing

Production system Firewall rules/Security Groups shall be audited for changes by an automated system on an hourly basis. Changes to firewalls, or unrecognized firewall entries shall immediately alert the CTO, ISO, and Security Administrators. Issues that require action shall be tracked with a JIRA request in the SysAdmin project queue.

G. Internal System Performance/Availability Monitoring

A system to monitor the internal availability of production systems shall be implemented. The system shall monitor individual production server/service instances and shall alert the CTO, ISO, and systems administrators if degraded performance or availability is detected. Issues that require action shall be tracked with a JIRA request in the SysAdmin project queue.

H. External System Monitoring

An external monitoring system shall be implemented to monitor the externally facing production systems. The external system shall alert the CTO, ISO, and systems administrators in the event of an externally detectable performance degradation or service failure. Issues that require action shall be tracked with a JIRA request in the SysAdmin project queue.

I. Third Party Compliance Monitoring

On an annual basis, the ISO shall request from vendors that host production data, third-party security audits, SOC reports, or other pertinent audits or reports for review. This action of compliance monitoring shall be tracked in a JIRA issue opened in the SysAdmin queue.

J. Notification of Security Breaches

Keeper shall notify affected parties (both internal and third-party) of a security breach within 24 hours of detection of the breach. Notification will take place over e-mail unless alternate contact methods have been specified otherwise.

IV. INFORMATION SECURITY DEFINITIONS

Availability: Data or information is accessible and usable upon demand by an authorized person.
Confidentiality: Data or information is not made available or disclosed to unauthorized persons or processes.
Integrity: Data or information has not been altered or destroyed in an unauthorized manner.
Involved Persons: Every worker at Keeper Security Inc. -- no matter what their status. This includes employees, contractors, consultants, temporaries, volunteers, interns, etc.
Involved Systems: All computer equipment and network systems that are operated within the Keeper Security Inc. environment. This includes all platforms (operating systems), all computer sizes (personal digital assistants, desktops, mainframes, etc.), and all applications and data (whether developed in-house or licensed from third parties) contained on those systems.
Protected Customer Data (PCD): PCD is data that is generated and stored by customer users. This can include personal data, passwords, name, e-mail, account information, or any other type of data a customer user may store using services or products offered by Keeper Security Inc. PCD also includes keys, passwords, certificates, or other information that permits decryption or access to PCD. For further information see the DATA CLASSIFICATION POLICY.
Risk: The probability of a loss of confidentiality, integrity, or availability of information resources.

V. INFORMATION SECURITY RESPONSIBILITIES

A. Information Security Officer

The Information Security Officer (ISO) is responsible for working with user management, owners, custodians, and users to develop and implement prudent security policies, procedures, and controls, subject to the approval of Keeper Security Inc. senior management. The Information Security Officer must report directly to senior management. Placing the ISO and InfoSec team outside of the typical hierarchical structure of the organization

is essential to removing conflicts of interest and enables objectivity in the execution of security policies, security planning, and security practices throughout the company. The ISO or any member of the Information Security (InfoSec) team may not be a member of any other role or entity listed outside of Section V., subsection A of this policy. Elements of security management planning include defining security roles; prescribing how security will be managed, who will be responsible for security, and how security will be tested for effectiveness; developing security policies; performing risk analysis; and requiring security education for employees. These efforts are guided through the development of management plans.

Specific responsibilities of the Information Security Office and InfoSec team include:

1. Ensuring security policies, plans, procedures, and standards are in place and adhered to by entity.

2. Providing basic security support for all systems and users, including management of firewalls, security monitoring/SIEM systems, access-lists, and access to system management portals and systems.

3. Advising owners in the identification and classification of computer resources. See Section VI Information Classification.

4. Advising systems development and application owners in the implementation of security controls for information on systems, from the point of system design, through testing and production implementation.

5. Educating information owner and user management with comprehensive information about security controls affecting system users and application systems.

6. Providing ongoing employee security education.

7. Performing security audits.

8. Determine if an exception to the security policy when an exception request is made in writing. Exceptions may include temporary changes to firewalls to permit external employee access during an emergency, or shared user accounts for services or software where it is not possible or practical to provide individual accounts to internal users. An exception may be granted if the request is deemed necessary and nature of the exception does not significantly expose the company to security risk.

9. Maintaining the Developer Role Chart which identifies individual Product Owners of the company's products and services.

10. Provides leadership and guidance for the Information Security (InfoSec) team/department.

11. Act as or delegate responsibilities as a designated Chief Information Security Officer (CISO), Chief Security Officer (CSO), Data Protection Officer (DPO) for the purposes of compliance with SOX, GDPR, or other compliance/certification purposes.

Keeper Security Inc. management who supervise users as defined below. User management is responsible for overseeing their employees' use of information, including:

12. Reviewing and approving all requests for their employees access authorizations.

13. Initiating security change requests to keep employees' security record current with their positions and job functions.

14. Promptly informing appropriate parties of employee terminations and transfers, in accordance with local entity termination procedures.

15. Revoking physical access to terminated employees, i.e., confiscating keys, changing combination locks, etc.

16. Providing employees with the opportunity for training needed to properly use the computer systems.

B. Systems Management (Data Custodians)

Systems Management is responsible for management of customer facing Production servers, networks, and associated services. The responsibilities of Systems Management include:

1. Deployment of approved hardware, software changes to customer-facing production servers and services, in accordance with the Change Control Procedure.

2. Maintaining and executing procedures for the management of business-critical production systems.

3. Responding to and resolving incidents that affect the availability of business-critical production systems.

4. Deploying software/hardware updates to maintain production system stability and security.

5. Initiating corrective actions to production systems when problems are identified.

6. Responsible for ongoing maintenance, performance/availability monitoring, capacity planning, and availability of informations systems to ensure that all internal and external service level commitments are met.

C. Product/Data Owners

The owner of a collection of information is usually the manager responsible for the creation of that information or the primary user of that information. This role often corresponds with the management of an organizational unit.

The owner of information has the responsibility for:

1. Knowing the information for which owner is responsible.

2. Determining a data retention period for the information.

3. Ensuring appropriate procedures are in effect to protect the integrity, confidentiality, and availability of the information used.

4. Specifying controls and communicating the control requirements to the internal users of the information.

5. Reporting promptly to the ISO the loss or misuse of Keeper Security Inc. information and initiating procedures according to the incident response plan.

6. Initiating corrective actions when problems are identified.

7. Promoting employee education and security awareness by utilizing programs approved by the ISO, where appropriate.

8. Approving changes to code that affect the availability of information in Keeper Security products and services, and implementing procedures for change control.

D. Internal User

The employee/internal user is any person who has been authorized to read, enter, or update information - this also applies to all users defined in sections A, B, C of this section. A user of information is expected to:

1. Access information only in support of their authorized job responsibilities.

2. Comply with Information Security Policies and Standards and with all controls established by the owner.

3. Keep personal authentication devices (e.g. passwords, SecureCards, PINs, etc.) confidential.

4. Report promptly to the ISO the loss or misuse of Keeper Security Inc. information.

5. Initiate corrective actions when problems are identified.

VI. COMPUTER AND INFORMATION CONTROL

A. Ownership of Software

All computer software developed by Keeper Security Inc. employees or contract personnel on behalf of Keeper Security Inc. or licensed for Keeper Security Inc. use is the property of Keeper Security Inc. and must not be copied for use at home or any other location, unless otherwise specified by the license agreement.

B. Installed Software

All software packages that reside on computers and networks within Keeper Security Inc. must comply with applicable licensing agreements and restrictions and must comply with Keeper Security Inc. acquisition of software policies.

C. Virus Protection and Endpoint Security Management

Endpoint Security Management and Virus Protection systems approved by the Information Security Officer and Information Services must be deployed using a multi-layered approach (desktops, servers, gateways, etc.) that ensures all electronic files are appropriately scanned for viruses and endpoints are protected from malicious software or processes. Users are not authorized to turn off or disable virus checking systems.

D. Audit Controls

Hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use PCD must be implemented. Further, procedures must be implemented to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

E. Contingency Planning

Controls must ensure that Keeper Security Inc. can recover from any damage to computer equipment or files within a reasonable period of time. System Management must develop and maintain a plan for responding to a system emergency or other occurrence (for example, fire, vandalism, system failure and natural disaster) that damages systems that contain PCD, Confidential, or Internal Information. This will include developing policies and procedures to address the following:

1. Data Backup Plan:
   a. Data backup plan must be documented and routinely updated to createand maintain, for a specific period of time, retrievable exact copies of information.

   b. Backup data must be stored in an off-site location and protected from physical damage

   c. Backup data must be afforded the same level of protection as the original data.

2. Disaster Recovery Plan

A disaster recovery plan must be developed and documented which contains a process enabling the entity to restore any loss of data in the event of fire, vandalism, natural disaster, or system failure.

3. Incident Response Plan

A plan must be developed to plan how the organization responses to breaches of security, unauthorized disclosure of PCD, Confidential Information, or Internal Information.

4. Business Continuity Plan

A plan shall be developed and maintained to ensure the continuation of business processes in the event of an incident that disrupts normal business operations at one or more office or data-center locations.

5. Patch Management

All IT Resources must be part of a patch management cycle. Available patches must be evaluated and applied to IT Resources every 90 days or less. Resources owners and managers are responsible for the assessment of IT Resources under their management or supervision. Patches that mitigate serious or critical vulnerabilities must be deployed as soon as possible using the Change Control Process.

VII. Physical Security

A. Physical Access Control

Physical access to Keeper Security business spaces shall be protected by doors that remain locked by default on a 24x7 basis. External access to business spaces shall be granted to authorized individuals via physical key, PIN code, RFID card, or by other secure electronic means.

B. Need of Access

Access shall be granted to areas based on business function. Employees shall be granted access to areas required for their work function.

The following areas shall be further restricted to those with a need for access:

- Server, Communications, Telephone Service Rooms
- Storage or supply rooms or closets
- Labs and Separated team workspaces
- Offices containing sensitive information

C. Visitors

Non-employee visitors must sign-in at the reception area of each office and issued a badge identifying the person as a visitor. This badge must be displayed at or above the belt line. Visitors shall be advised of the areas that they are to be accompanied by an escort.

D. Surveillance and Logging

24x7 camera surveillance shall be installed to monitor all egress and ingress points of the business space. The surveillance footage shall be recorded to a DVR or similar storage device and remain reviewable for up to 7 days.

VIII. Compliance

A. Non-Compliance

Breaches and non-compliance of this policy may be treated as a disciplinary matter dealt with under disciplinary procedures as defined in the Employee Handbook. Where third parties are involved breach of this policy may also constitute breach of contract.

Addendum F

SCHEDULE OF DATA

Category of Data	Elements	Check if used by your system
Application Technology Meta Data	IP Addresses, Use of cookies etc.	X
	Other application technology meta data Specify:	
Application Use Statistics	Meta data on user interaction with application	
Assessment	Standardized test scores	
	Observation data	
	Other assessment data (specify): *Student Personality Assessments*	
Attendance	Student school (daily) attendance data	
	Student class attendance data	
Communications	Online communications that are captured (emails, blog entries)	
Conduct	Conduct or behavioral data	
Demographics	Date of Birth	
	Place of Birth	
	Gender	
	Ethnicity or race	
	Language information (native, preferred or primary language spoken by student)	
	Other demographic information Specify:	
Enrollment	Student school enrollment	
	Student grade level	
	Homeroom	
	Guidance counselor	
	Specific curriculum programs	
	Year of graduation	
	Other enrollment information (specify):	
Parent/Guardian Contact Information	Address	
	Email	
	Phone	
Parent/Guardian ID	Parent ID number (created to link parents to students)	
Parent/Guardian Name	First and/or Last	
Schedule	Student scheduled courses	

Category of Data	Elements	Check if used by your system
	Teacher names	
Special Indicator	English language learner information	
	Low income status	
	Medical alerts	
	Student disability information	
	Specialized education services (IEP or 504)	
	Living situations (homeless/foster care)	
	Other indicator information(specify): *First Generation College Student*	
Student Contact Information	Address	
	Email	
	Phone	
Student Identifiers	Local (School district) ID number	
	State ID number	
	Vendor/App assigned student ID No.	
	Student app username	
	Student app passwords	
Student Name	First and/or Last	
Student In-App Performance	Program/application performance (typing program-student types 60 wpm, reading program-student reads below grade level)	
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	
Student Survey Responses	Student responses to surveys or questionnaires	
Student work	Student generated content; writing, pictures etc.	
	Other student work data Please specify:	
Transcript	Student course grades	
	Student course data	
	Student course grades/performance scores	
	Other transcript data Please specify:	
	Student bus assignment	

Category of Data	Elements	Check if used by your system
Transportation	Student pick up and/or drop off location	
	Student bus card ID number	
	Other transportation data Please specify:	
Other	Please list each additional data element used, stored or collected by your application	

Addendum G

JOINDER AGREEMENT

This Joinder Agreement ("Joinder") is effective as of the date of signature below and is entered into by the undersigned Participating School pursuant to that certain Agreement, dated October 1, 2021 by and between Keeper Security, Inc. and Phoenix Central School District (the "Agreement"). Capitalized terms used but not defined in this Joinder shall have the respective meanings ascribed to such terms in the Agreement. By the execution of this Joinder, the Participating School (i) agrees to be bound by, and subject to, the terms and conditions of the Agreement as a "Participating School" and a "Party" thereunder, (ii) adopts the Agreement with the same force and effect as if the Participating School was originally a party thereto, and (iii) agrees that any Confidential Data provided by the Participating School to Vendor shall be governed by the Agreement.

The Agreement shall extend only to the data privacy and security matters that are the subject matter thereof and the Terms shall continue to govern with respect to all other matters. In the event of a conflict or an inconsistency between the terms and conditions of the Terms and the terms and conditions of the Agreement, the Agreement shall govern and control.

In order for this Joinder to be effective, the Participating School must send a signed copy of this Joinder to Phoenix Central School District via email to mfoley@phoenixcsd.org or by mail to Michael Foley, Director of Data and Instructional Technology, Phoenix Central School District, 116 Volney Street, Phoenix, NY 13135 and to Vendor via email at njamison@keepersecurity.com or by mail to Attn: Legal, 820 W. Jackson Blvd., Suite 400 Chicago, IL 60607.

Name of Participating School:

By: _____

Name: _____

Title: _____

Date: _____

Address: _____

_____