AGREEMENT
REGARDING DATA SECURITY AND PRIVACY

This Agreement regarding Data Security and Privacy ("Agreement") dated as of April 10, 2024, by and between the Norwood-Norfolk Central School District ("District") and CK-12 Foundation ("Contractor"). This Agreement covers only student accounts sanctioned by the district and set up through the nncsk12.org and students.nncsk12.org domain(s).

WHEREAS, the District has licensed certain services or products from Contractor, pursuant to and as identified in Contractor's Terms of Use, found at www.ck12info.org/about/terms-of-use/ ("Contractor TOU"), which is incorporated herein as may be amended; and

WHEREAS, Contractor is a third-party contractor as defined in Part 121 of the Commissioner's Regulations, that will receive student data or teacher or principal data from the District pursuant to "Contractor TOU," and this Agreement for purposes of providing services to the District; and

WHEREAS, the parties agree that if any provision of this Agreement conflicts with a provision of "Contractor TOU," the provision as set forth in this Agreement shall supersede and prevail over said other provision;

NOW, THEREFORE, in consideration of the mutual covenants, conditions and agreements contained herein, and for other good and valuable consideration, including the above-referenced "Contractor TOU," the Contractor and the District hereby agree as follows:

A. The Contractor shall comply with all state, federal, and local laws, regulations, rules, and requirements related to the confidentiality of records and data security and privacy, including the Parents' Bill of Rights, hereinafter referred to as "Attachment A," and Supplemental Information, annexed hereto and herein after referred to as "Attachment B."

B. The Contractor may receive personally identifiable information from student records ("Education Records") and/or personally identifiable information from annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release pursuant to Education Law § 3012-c and 3012-d (collectively, "PII Data"). The Contractor shall, therefore, comply with the following provisions in order to maintain the security and confidentiality of personally identifiable information:

(i) adopt technologies, safeguards and practices in alignment with the NIST Cybersecurity Framework;
(ii) limit the Contractor's internal access to Education Records to individuals with legitimate educational interests;
(iii) use PII Data only for the purposes explicitly authorized by this Agreement and not for any other purpose;
(iv) not disclose any personally identifiable information from PII Data to any other party without prior written consent, unless disclosure is required by statute or court order and written notice is given to the District (notice is not required if it is

expressly prohibited by a statute or court order);

(v) maintain reasonable safeguards to maintain confidentiality of personally identifiable information in PII Data;

(vi) use legally mandated encryption technology[1] to protect data from unauthorized disclosure while the data is in motion or in the contractor's custody; and

(vii) not sell, use or disclose student, teacher or principal personally identifiable information for any marketing or commercial purpose.

(viii) For the avoidance of doubt, it is expressly understood and agreed that Education Records do not include students' "User Content," as defined in the "Contractor TOU."

C. The Contractor represents and warrants that it will follow and abide by the guidelines and legal standards as set forth in the Contractor's data security and privacy plan as attached hereto as "Attachment C."

The Contractor's data security and privacy plan shall, at a minimum:

(i) outline how the Contractor will implement State and federal data security and privacy contract requirements for the life of the contract;

(ii) specify administrative, operational and technical safeguards the third-party contractor will use to protect personally identifiable information;

(iii) show that it complies with requirements of §121.3(c) of the Commissioner's Regulations;

(iv) specify how the third-party contractor's employees and any assignees with access to student data, or teacher or principal data receive or will receive training on relevant confidentiality laws, before receiving access to such data;

(v) specify if the third-party contractor will use subcontractors and how it will ensure personally identifiable information is protected;

(vi) specify an action plan for handling any breach or unauthorized disclosure of personally identifiable information and promptly notify the school district of any breach or unauthorized disclosure; and

(vii) describe whether, how and when data will be returned, transitioned to a successor contractor, deleted or destroyed when the contract ends or is terminated.

D. The Contractor must notify the District of any breach of security resulting in an unauthorized release of personally identifiable information from PII Data by the Contractor or the Contractor's officers, employee's, assignees or subcontractors. This notification must be made in the most expedient way possible and without delay. In addition, the Contractor must notify the District of the breach of security in writing. This written notification must be sent by the Contractor in the most expedient way possible and without unreasonable delay, and not later than seven (7) calendar days after confirmation of the breach of security resulting in an unauthorized release of personally identifiable information from PII Data, to the designated District representative and will be delivered to the District by electronic mail to James

[1] Encryption means methods of rendering personally identifiable information unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified or permitted by the Secretary of the United States department of health and human services in guidance issued under Section 13402(H)(2) of Public Law 111-5.

Cruikshank, Superintendent, jcruikshank@nncsk12.org. In the case of an unauthorized release of personally identifiable information from PII Data by the Contractor or the Contractor's officers, employees, assignees or subcontractors, the Contractor will reimburse the District for the reasonable cost to fulfill the District's obligation to notify any required party pursuant to NYCRR 121.10(f), subject to any limitation of liability agreed to in Contractor's TOU. For the avoidance of doubt, this reimbursement obligation does not include any other costs or losses related to responding to a breach of security (e.g. District legal fees, notification under other statutes).

E. The Contractor and District agree that this Agreement and the Attachments included hereto supersede and replace any previous agreements or contracts between the parties.

IN WITNESS WHEREOF, the parties hereto have set their respective hands and seals as of the date and year first above written.

DISTRICT: Norwood-Norfolk Central School District	CONTRACTOR: CK-12 Foundation
BY: James Cruikshank, Superintendent James Cruikshank James Cruikshank (Apr 10, 2024 13:07 EDT)	BY: Miral Shah, Chief Technology & Product Officer DocuSigned by: Miral Shah 81C4BF5FA8444CF...
DATE: Apr 10, 2024	DATE: 6/11/2024

ATTACHMENT A

PARENTS' BILL OF RIGHTS FOR STUDENT 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 should be directed to: James Cruikshank, Superintendent, jcruikshank@nncsk12.org. Complaints may also be submitted to NYSED at http://www.nysed.gov/data-privacysecurity/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.

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.

ATTACHMENT B
PARENTS' BILL OF RIGHTS FOR
STUDENT DATA PRIVACY AND SECURITY
THIRD PARTY CONTRACTOR SUPPLEMENT

In accordance with its obligations under the Parents' Bill Rights and Data Privacy and Security Agreement, the Contractor verifies the following supplemental information to the Parents' Bill of Rights regarding data privacy and security:

(1) The student data or teacher or principal data (collectively, "PII Data") received by the Contractor will be used exclusively for the following purpose(s):

Contractor and its agents, employees and subcontractors, if any, shall use PII Data solely for the purpose of providing services as set forth in the "Contractor TOU," and this Agreement. Contractor and its agents, employees and subcontractors will not use PII Data for any other purposes. Any Data received by Contractor or any of its agents, employees, subcontractors or assignees shall not be sold or released for any commercial purposes, nor shall it be sold or used for marketing purposes.

(2) The Contractor will ensure the confidentiality of PII Data that is shared with subcontractors or other persons or entities as follows:

In the event that Contractor subcontracts with an outside entity or individual in order to fulfill its obligations to the District, Contractor ensures that it will only share PII Data with such subcontractors as described as "Third Party Service Providers" in "Attachment C" section (v) who maintain such data privacy and security consistent with those required of Contractor pursuant to the Agreement. Contractor will maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of PII Data in its custody consistent with the data protection and security requirements of state and federal law and regulations by adhering to the provisions in the "THIRD-PARTY CONTRACTOR'S DATA SECURITY AND PRIVACY PLAN," "Attachment C."

(3) This Agreement is effective upon execution by both parties and shall continue until terminated by either party by giving at least 30 days written notice. Within thirty (30) calendar days after the termination of the Agreement, all PII Data will be de-identified and/or deleted from Contractor's computer systems, based on written request from the District. Contractor will provide written confirmation of such disposition to the District, upon written request.

(4) A parent, student, teacher or principal can challenge the accuracy of PII Data received by the Contractor as follows:

In the event that a parent or eligible student wishes to challenge the accuracy of PII Data concerning that student that is maintained by Contractor or its subcontractors, such challenge may be processed through the procedures provided by the applicable educational agency or institution for amendment of education records under the Family Educational Rights and Privacy Act (FERPA). In the event that Contractor is notified of the outcome of any such

errors made by Contractor, it will promptly correct any inaccurate data it or its subcontractors or assignees maintain. The District or the applicable New York education agency/institution will use FERPA's data correction procedures, as applicable, to update any data that is not a result of an error made by Contractor or its subcontractors.

(5) The following is how PII Data will be stored and what security protections will be taken by the Contractor:

All Data in Contractor's possession will be securely stored. Contractor represents that the following security protections, including encryption where applicable, will be in place to ensure that PII Data is protected.

- Password protections
- Administrative procedures
- Encryption while PII is in motion and at rest
- Firewalls

ATTACHMENT C
THIRD-PARTY CONTRACTOR'S DATA SECURITY AND PRIVACY PLAN

In accordance with its obligations under the Parents' Bill Rights and Data Privacy and Security Agreement, the Contractor represents and warrants that its data security and privacy plan described below or attached hereto contains the following minimum required provisions:

(i) Contractor will implement State and federal data security and privacy contract requirements for the duration of its contract by:

Adhering to the NIST Cybersecurity Framework. Our NIST "Current Profile" is available upon request.

(ii) Contractor will use the following administrative, operational and technical safeguards to protect personally identifiable information:

Refer to Section 11 of the CK-12 Privacy Policy, found at https://www.ck12info.org/privacy-policy/

(iii) Contractor has complied with requirements of §121.3(c) of the Commissioner's Regulations by providing and complying with the supplemental contractor information as follows:

§121.3(c)(1)
- Refer to Section 5 in the CK-12 Privacy Policy, found at https://www.ck12info.org/privacy-policy/

§121.3(c)(2)
- Refer to Section 6 in the CK-12 Privacy Policy, found at https://www.ck12info.org/privacy-policy/

§121.3(c)(3)
- For contract duration, refer to item 3 in the Supplement to the Parents' Bill of Rights, "Attachment B," above.
- For disposition or transfer of data, refer to item 3 in the Supplement to the Parents' Bill of Rights, "Attachment B," above, and to Sections 8 and 13 in the CK-12 Privacy Policy, found at https://www.ck12info.org/privacy-policy/

§121.3(c)(4)
- Refer to item 4 in the Parents' Bill of Rights above.

§121.3(c)(5)
- The CK-12 site runs on the Amazon Web Services (AWS) cloud.
- Refer to Section 13 in the CK-12 Privacy Policy, found at

https://www.ck12info.org/privacy-policy/, for more information on security.

§121.3(c)(6)
- Refer to Section 13 in the CK-12 Privacy Policy, found at https://www.ck12info.org/privacy-policy/

(iv) Contractor's employees and any assignees with access to student data, or teacher or principal data have received or will receive training on relevant confidentiality laws, before receiving access to such data, as follows:

Employees with access to PII receive training on handling this data.

(v) Contractor works with third party service providers for cloud-based hosting, communicating with users for product support and information, troubleshooting issues, and analytics.

For more information on any of the third parties used by Contractor, please email: support@ck12.org

(vi) Contractor will implement an action plan for handling any breach or unauthorized disclosure of personally identifiable information and will promptly notify the school district of any breach or unauthorized disclosure as follows:

CK-12 has an established incident response plan, which can be provided upon request.

(vii) Data will be returned, transitioned to a successor contractor, deleted, de-identified, or destroyed when the contract ends or is terminated as follows:

- For disposition or transfer of data, refer to item 3 in the Supplement to the Parents' Bill of Rights, "Attachment B," above, and to Section 6 in the CK-12 Privacy Policy, found at https://www.ck12info.org/privacy-policy/

Function	Category	Subcategory	Compliant	Notes	Informative References
		The following apply to both www.ck12.org and flexbooks.ck12.org.			
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	**ID.AM-1**: Physical devices and systems within the organization are inventoried	YES		· NIST SP 800-53 Rev. 4 CM-8
		ID.AM-2: Software platforms and applications within the organization are inventoried	YES		· NIST SP 800-53 Rev. 4 CM-8
		ID.AM-3: Organizational communication and data flows are mapped	YES		· NIST SP 800-53 Rev. 4 AC-4 · NIST SP 800-53 Rev. 4 CA-3 · NIST SP 800-53 Rev. 4 CA-9 · NIST SP 800-53 Rev. 4 PL-8
		ID.AM-4: External information systems are catalogued	YES		· NIST SP 800-53 Rev. 4 AC-20 · NIST SP 800-53 Rev. 4 SA-9
		ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	YES		· NIST SP 800-53 Rev. 4 CP-2 · NIST SP 800-53 Rev. 4 RA-2 · NIST SP 800-53 Rev. 4 SA-14
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	YES		· NIST SP 800-53 Rev. 4 CP-2 · NIST SP 800-53 Rev. 4 PS-7 · NIST SP 800-53 Rev. 4 PM-11
	Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	**ID.BE-1:** The organization's role in the supply chain is identified and communicated	N/A	We believe this doesn't apply to us, since we don't have a supply chain in the traditional sense.	· NIST SP 800-53 Rev. 4 CP-2 N/A?
		ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	N/A	We believe this doesn't apply to us, since we are not part of a supply chain in the traditional sense.	· NIST SP 800-53 Rev. 4 PM-8
		ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	YES		· NIST SP 800-53 Rev. 4 PM-11 · NIST SP 800-53 Rev. 4 SA-14
		ID.BE-4: Dependencies and critical functions for delivery of critical services are established	YES		· NIST SP 800-53 Rev. 4 CP-8 · NIST SP 800-53 Rev. 4 PE-9 · NIST SP 800-53 Rev. 4 PE-11 · NIST SP 800-53 Rev. 4 PM-8 · NIST SP 800-53 Rev. 4 SA-14
		ID.BE-5: Resilience requirements to support delivery of critical services are established	YES		· NIST SP 800-53 Rev. 4 CP-2 · NIST SP 800-53 Rev. 4 CP-11 · NIST SP 800-53 Rev. 4 SA-14
	Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	**ID.GV-1:** Organizational information security policy is established	YES		· NIST SP 800-53 Rev. 4 -1 controls from all families
		ID.GV-2: Information security roles & responsibilities are coordinated and aligned with internal roles and external partners	YES		· NIST SP 800-53 Rev. 4 PM-1 · NIST SP 800-53 Rev. 4 PS-7
		ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	YES		· NIST SP 800-53 Rev. 4 -1 controls from all families (except PM-1)
		ID.GV-4: Governance and risk management processes address cybersecurity risks	YES		· NIST SP 800-53 Rev. 4 PM-9 · NIST SP 800-53 Rev. 4 PM-11
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	**ID.RA-1:** Asset vulnerabilities are identified and documented	YES		· NIST SP 800-53 Rev. 4 CA-2 · NIST SP 800-53 Rev. 4 CA-7 · NIST SP 800-53 Rev. 4 CA-8 · NIST SP 800-53 Rev. 4 RA-3 · NIST SP 800-53 Rev. 4 RA-5 · NIST SP 800-53 Rev. 4 SA-5 · NIST SP 800-53 Rev. 4 SA-11 · NIST SP 800-53 Rev. 4 SI-2 · NIST SP 800-53 Rev. 4 SI-4 · NIST SP 800-53 Rev. 4 SI-5

		ID.RA-2: Threat and vulnerability information is received from information sharing forums and sources	**YES**		· NIST SP 800-53 Rev. 4 PM-15 · NIST SP 800-53 Rev. 4 PM-16 · NIST SP 800-53 Rev. 4 SI-5
		ID.RA-3: Threats, both internal and external, are identified and documented	**YES**		· NIST SP 800-53 Rev. 4 RA-3 · NIST SP 800-53 Rev. 4 PM-12 · NIST SP 800-53 Rev. 4 PM-16
		ID.RA-4: Potential business impacts and likelihoods are identified	**YES**		· NIST SP 800-53 Rev. 4 RA-2 · NIST SP 800-53 Rev. 4 RA-3 · NIST SP 800-53 Rev. 4 PM-9 · NIST SP 800-53 Rev. 4 PM-11 · NIST SP 800-53 Rev. 4 SA-14
		ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	**YES**		· NIST SP 800-53 Rev. 4 RA-2 · NIST SP 800-53 Rev. 4 RA-3 · NIST SP 800-53 Rev. 4 PM-16
		ID.RA-6: Risk responses are identified and prioritized	**YES**		· NIST SP 800-53 Rev. 4 PM-4 · NIST SP 800-53 Rev. 4 PM-9
	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	**ID.RM-1:** Risk management processes are established, managed, and agreed to by organizational stakeholders	**YES**		· NIST SP 800-53 Rev. 4 PM-9
		ID.RM-2: Organizational risk tolerance is determined and clearly expressed	**YES**		· NIST SP 800-53 Rev. 4 PM-9
		ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis	**YES**		· NIST SP 800-53 Rev. 4 PM 8 · NIST SP 800-53 Rev. 4 PM-9 · NIST SP 800-53 Rev. 4 PM-11 · NIST SP 800-53 Rev. 4 SA-14
PROTECT (PR)	**Access Control (PR.AC):** Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	**PR.AC-1:** Identities and credentials are managed for authorized devices and users	**YES**		· NIST SP 800-53 Rev. 4 AC-2 · NIST SP 800-53 Rev. 4 IA Family
		PR.AC-2: Physical access to assets is managed and protected	**YES**		· NIST SP 800-53 Rev. 4 PE-2 · NIST SP 800-53 Rev. 4 PE-3 · NIST SP 800-53 Rev. 4 PE-4 · NIST SP 800-53 Rev. 4 PE-5 · NIST SP 800-53 Rev. 4 PE-6 · NIST SP 800-53 Rev. 4 PE-9
		PR.AC-3: Remote access is managed	**YES**		· NIST SP 800-53 Rev. 4 AC-17 · NIST SP 800-53 Rev. 4 AC-19 · NIST SP 800-53 Rev. 4 AC-20
		PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties	**YES**		· NIST SP 800-53 Rev. 4 AC-2 · NIST SP 800-53 Rev. 4 AC-3 · NIST SP 800-53 Rev. 4 AC-5 · NIST SP 800-53 Rev. 4 AC-6 · NIST SP 800-53 Rev. 4 AC-16
		PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate	**YES**		· NIST SP 800-53 Rev. 4 AC-4 · NIST SP 800-53 Rev. 4 SC-7
	Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.	**PR.AT-1:** All users are informed and trained	**N/A**	Personnel who have security-related duties, or have access to PII recieve relevant training. This does not apply to all employees, so we have marked it as N/A.	· NIST SP 800-53 Rev. 4 AT-2 · NIST SP 800-53 Rev. 4 PM-13
		PR.AT-2: Privileged users understand roles & responsibilities	**YES**		· NIST SP 800-53 Rev. 4 AT-3 · NIST SP 800-53 Rev. 4 PM-13
		PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities	**N/A**	We don't have suppliers, per se. Relationships with service providers, such as AWS are defined by contracts. Relationships with users of the site are defined by our TOU. No training is necessary.	· NIST SP 800-53 Rev. 4 PS-7 · NIST SP 800-53 Rev. 4 SA-9
		PR.AT-4: Senior executives understand roles & responsibilities	**YES**		· NIST SP 800-53 Rev. 4 AT-3 · NIST SP 800-53 Rev. 4 PM-13
		PR.AT-5: Physical and information security personnel understand	**YES**		· NIST SP 800-53 Rev. 4 AT-3

		roles & responsibilities			· NIST SP 800-53 Rev. 4 PM-13
	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	**PR.DS-1:** Data-at-rest is protected	**YES**		· NIST SP 800-53 Rev. 4 SC-28
		PR.DS-2: Data-in-transit is protected	**YES**		· NIST SP 800-53 Rev. 4 SC-8
		PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition	**YES**		· NIST SP 800-53 Rev. 4 CM-8 · NIST SP 800-53 Rev. 4 MP-6 · NIST SP 800-53 Rev. 4 PE-16
		PR.DS-4: Adequate capacity to ensure availability is maintained	**YES**		· NIST SP 800-53 Rev. 4 AU-4 · NIST SP 800-53 Rev. 4 CP-2 · NIST SP 800-53 Rev. 4 SC-5
		PR.DS-5: Protections against data leaks are implemented	**YES**		· NIST SP 800-53 Rev. 4 AC-4 · NIST SP 800-53 Rev. 4 AC-5 · NIST SP 800-53 Rev. 4 AC-6 · NIST SP 800-53 Rev. 4 PE-19 · NIST SP 800-53 Rev. 4 PS-3 · NIST SP 800-53 Rev. 4 PS-6 · NIST SP 800-53 Rev. 4 SC-7 · NIST SP 800-53 Rev. 4 SC-8 · NIST SP 800-53 Rev. 4 SC-13 · NIST SP 800-53 Rev. 4 SC-31 · NIST SP 800-53 Rev. 4 SI-4
		PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	**TARGET PROFILE ITEM**	We are not currently doing this, in an automated way but belive it makes sense to implement. We have detailed proposed changes in our internal Configuration Management document. We also do cover some of this functionality through QA and operations processes, but not enough to consider this item fully implemented.	· NIST SP 800-53 Rev. 4 SI-7
		PR.DS-7: The development and testing environment(s) are separate from the production environment	**YES**		· NIST SP 800-53 Rev. 4 CM-2
	Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	**PR.IP-1:** A baseline configuration of information technology/industrial control systems is created and maintained	**YES**		· NIST SP 800-53 Rev. 4 CM-2 · NIST SP 800-53 Rev. 4 CM-3 · NIST SP 800-53 Rev. 4 CM-4 · NIST SP 800-53 Rev. 4 CM-5 · NIST SP 800-53 Rev. 4 CM-6 · NIST SP 800-53 Rev. 4 CM-7 · NIST SP 800-53 Rev. 4 CM-9 · NIST SP 800-53 Rev. 4 SA-10
		PR.IP-2: A System Development Life Cycle to manage systems is implemented	**N/A**	Since we outsource hosting for our application to AWS, we believe this doesn't apply to us. We do have a defined and documented Software Development Lifecycle, which governs how we bring new features to production. However, this subcategory seems to apply more to the general infrastructure supporting the application.	· NIST SP 800-53 Rev. 4 SA-3 · NIST SP 800-53 Rev. 4 SA-4 · NIST SP 800-53 Rev. 4 SA-8 · NIST SP 800-53 Rev. 4 SA-10 · NIST SP 800-53 Rev. 4 SA-11 · NIST SP 800-53 Rev. 4 SA-12 · NIST SP 800-53 Rev. 4 SA-15 · NIST SP 800-53 Rev. 4 SA-17 · NIST SP 800-53 Rev. 4 PL-8
		PR.IP-3: Configuration change control processes are in place	**YES**		· NIST SP 800-53 Rev. 4 CM-3 · NIST SP 800-53 Rev. 4 CM-4 · NIST SP 800-53 Rev. 4 SA-10
		PR.IP-4: Backups of information are conducted, maintained, and tested periodically	**YES**		· NIST SP 800-53 Rev. 4 CP-4 · NIST SP 800-53 Rev. 4 CP-6 · NIST SP 800-53 Rev. 4 CP-9

		PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met	**YES**		· NIST SP 800-53 Rev. 4 PE-10 · NIST SP 800-53 Rev. 4 PE-12 · NIST SP 800-53 Rev. 4 PE-13 · NIST SP 800-53 Rev. 4 PE-14 · NIST SP 800-53 Rev. 4 PE-15 · NIST SP 800-53 Rev. 4 PE-18
		PR.IP-6: Data is destroyed according to policy	**YES**		· NIST SP 800-53 Rev. 4 MP-6
		PR.IP-7: Protection processes are continuously improved	**YES**		· NIST SP 800-53 Rev. 4 CA-2 · NIST SP 800-53 Rev. 4 CA-7 · NIST SP 800-53 Rev. 4 CP-2 · NIST SP 800-53 Rev. 4 IR-8 · NIST SP 800-53 Rev. 4 PL-2 · NIST SP 800-53 Rev. 4 PM-6
		PR.IP-8: Effectiveness of protection technologies is shared with appropriate parties	**N/A**	There is no one externally with whom we would need to share this. Much of the protection technologies in use are implemented by AWS.	· NIST SP 800-53 Rev. 4 AC-21 · NIST SP 800-53 Rev. 4 CA-7 · NIST SP 800-53 Rev. 4 SI-4
		PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	**YES**		· NIST SP 800-53 Rev. 4 CP-2 · NIST SP 800-53 Rev. 4 IR-8
		PR.IP-10: Response and recovery plans are tested	**YES**		· NIST SP 800-53 Rev. 4 CP-4 · NIST SP 800-53 Rev.4 IR-3 · NIST SP 800-53 Rev.4 PM-14
		PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	**YES**		· NIST SP 800-53 Rev. 4 PS Family
		PR.IP-12: A vulnerability management plan is developed and implemented	**YES**		· NIST SP 800-53 Rev. 4 RA-3 · NIST SP 800-53 Rev. 4 RA-5 · NIST SP 800-53 Rev. 4 SI-2
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.	**PR.MA-1:** Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools	**YES**		· NIST SP 800-53 Rev. 4 MA-2 · NIST SP 800-53 Rev. 4 MA-3 · NIST SP 800-53 Rev. 4 MA-5
		PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents	**YES**		· NIST SP 800-53 Rev. 4 MA-4
	Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	**PR.PT-1:** Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	**Yes**		· NIST SP 800-53 Rev. 4 AU Family
		PR.PT-2: Removable media is protected and its use restricted according to policy	**TARGET PROFILE ITEM**	CK-12 does not provide removable media such as external drives, smart phones, etc. However, since it is possible that employees with access could put PII on their own media we will educate employees that this would be contrary to CK-12 policy. We will do so initially by email, and also eventually add this to our Employee Handbook.	· NIST SP 800-53 Rev. 4 MP-2 · NIST SP 800-53 Rev. 4 MP-4 · NIST SP 800-53 Rev. 4 MP-5 · NIST SP 800-53 Rev. 4 MP-7
		PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality	**YES**		· NIST SP 800-53 Rev. 4 AC-3 · NIST SP 800-53 Rev. 4 CM-7
		PR.PT-4: Communications and control networks are protected	**YES**		· NIST SP 800-53 Rev. 4 AC-4 · NIST SP 800-53 Rev. 4 AC-17 · NIST SP 800-53 Rev. 4 AC-18 · NIST SP 800-53 Rev. 4 CP-8 · NIST SP 800-53 Rev. 4 SC-7
DETECT (DE)	**Anomalies and Events (DE.AE):** Anomalous activity is detected in a timely manner and the potential impact of events is understood.	**DE.AE-1:** A baseline of network operations and expected data flows for users and systems is established and managed	**YES**		· NIST SP 800-53 Rev. 4 AC-4 · NIST SP 800-53 Rev. 4 CA-3 · NIST SP 800-53 Rev. 4 CM-2 · NIST SP 800-53 Rev. 4 SI-4
		DE.AE-2: Detected events are analyzed to understand attack targets and methods	**YES**		· NIST SP 800-53 Rev. 4 AU-6 · NIST SP 800-53 Rev. 4 CA-7 · NIST SP 800-53 Rev. 4 IR-4 · NIST SP 800-53 Rev. 4 SI-4
		DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors	**YES**		· NIST SP 800-53 Rev. 4 AU-6 · NIST SP 800-53 Rev. 4 CA-7

					· NIST SP 800-53 Rev. 4 IR-4 · NIST SP 800-53 Rev. 4 IR-5 · NIST SP 800-53 Rev. 4 IR-8 · NIST SP 800-53 Rev. 4 SI-4
		DE.AE-4: Impact of events is determined	**YES**		· NIST SP 800-53 Rev. 4 CP-2 · NIST SP 800-53 Rev. 4 IR-4 · NIST SP 800-53 Rev. 4 RA-3 · NIST SP 800-53 Rev. 4 SI-4
		DE.AE-5: Incident alert thresholds are established	**YES**		· NIST SP 800-53 Rev. 4 IR-4 · NIST SP 800-53 Rev. 4 IR-5 · NIST SP 800-53 Rev. 4 IR-8
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.	**DE.CM-1:** The network is monitored to detect potential cybersecurity events	**YES**		· NIST SP 800-53 Rev. 4 AC-2 · NIST SP 800-53 Rev. 4 AU-12 · NIST SP 800-53 Rev. 4 CA-7 · NIST SP 800-53 Rev. 4 CM-3 · NIST SP 800-53 Rev. 4 SC-5 · NIST SP 800-53 Rev. 4 SC-7 · NIST SP 800-53 Rev. 4 SI-4
		DE.CM-2: The physical environment is monitored to detect potential cybersecurity events	**YES**		· NIST SP 800-53 Rev. 4 CA-7 · NIST SP 800-53 Rev. 4 PE-3 · NIST SP 800-53 Rev. 4 PE-6 · NIST SP 800-53 Rev. 4 PE-20
		DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events	**YES**		· NIST SP 800-53 Rev. 4 AC-2 · NIST SP 800-53 Rev. 4 AU-12 · NIST SP 800-53 Rev. 4 AU-13 · NIST SP 800-53 Rev. 4 CA-7 · NIST SP 800-53 Rev. 4 CM-10 · NIST SP 800-53 Rev. 4 CM-11
		DE.CM-4: Malicious code is detected	**YES**		· NIST SP 800-53 Rev. 4 SI-3
		DE.CM-5: Unauthorized mobile code is detected	**YES**		· NIST SP 800-53 Rev. 4 SC-18 · NIST SP 800-53 Rev. 4 SI-4 · NIST SP 800-53 Rev. 4 SC-44
		DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events	**YES**		· NIST SP 800-53 Rev. 4 CA-7 · NIST SP 800-53 Rev. 4 PS-7 · NIST SP 800-53 Rev. 4 SA-4 · NIST SP 800-53 Rev. 4 SA-9 · NIST SP 800-53 Rev. 4 SI-4
		DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	**YES**		· NIST SP 800-53 Rev. 4 AU-12 · NIST SP 800-53 Rev. 4 CA-7 · NIST SP 800-53 Rev. 4 CM-3 · NIST SP 800-53 Rev. 4 CM-8 · NIST SP 800-53 Rev. 4 PE-3 · NIST SP 800-53 Rev. 4 PE-6 · NIST SP 800-53 Rev. 4 PE-20 · NIST SP 800-53 Rev. 4 SI-4
		DE.CM-8: Vulnerability scans are performed	**YES**		· NIST SP 800-53 Rev. 4 RA-5
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.	**DE.DP-1:** Roles and responsibilities for detection are well defined to ensure accountability	**YES**		· NIST SP 800-53 Rev. 4 CA-2 · NIST SP 800-53 Rev. 4 CA-7 · NIST SP 800-53 Rev.4 PM-14
		DE.DP-2: Detection activities comply with all applicable requirements	**YES**		· NIST SP 800-53 Rev. 4 CA-2 · NIST SP 800-53 Rev. 4 CA-7 · NIST SP 800-53 Rev. 4 SI-4 · NIST SP 800-53 Rev.4 PM-14
		DE.DP-3: Detection processes are tested	**YES**		· NIST SP 800-53 Rev. 4 CA-2 · NIST SP 800-53 Rev. 4 CA-7 · NIST SP 800-53 Rev. 4 PE-3

					· NIST SP 800-53 Rev.4 PM-14 · NIST SP 800-53 Rev. 4 SI-3 · NIST SP 800-53 Rev. 4 SI-4
		DE.DP-4: Event detection information is communicated to appropriate parties	**YES**		· NIST SP 800-53 Rev. 4 AU-6 · NIST SP 800-53 Rev. 4 CA-2 · NIST SP 800-53 Rev. 4 CA-7 · NIST SP 800-53 Rev. 4 RA-5 · NIST SP 800-53 Rev. 4 SI-4
		DE.DP-5: Detection processes are continuously improved	**YES**		· NIST SP 800-53 Rev. 4 CA-2 · NIST SP 800-53 Rev. 4 CA-7 · NIST SP 800-53 Rev. 4 PL-2 · NIST SP 800-53 Rev. 4 RA-5 · NIST SP 800-53 Rev. 4 SI-4 · NIST SP 800-53 Rev.4 PM-14
RESPOND (RS)	**Response Planning (RS.RP):** Response processes and procedures are executed and maintained, to ensure timely	**RS.RP-1:** Response plan is executed during or after an event	**YES**		· NIST SP 800-53 Rev. 4 CP-2 · NIST SP 800-53 Rev. 4 CP-10 · NIST SP 800-53 Rev. 4 IR-4 · NIST SP 800-53 Rev. 4 IR-8
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.	**RS.CO-1:** Personnel know their roles and order of operations when a response is needed	**YES**		· NIST SP 800-53 Rev. 4 CP-2 · NIST SP 800-53 Rev. 4 CP-3 · NIST SP 800-53 Rev. 4 IR-3 · NIST SP 800-53 Rev. 4 IR-8
		RS.CO-2: Events are reported consistent with established criteria	**YES**		· NIST SP 800-53 Rev. 4 AU-6 · NIST SP 800-53 Rev. 4 IR-6 · NIST SP 800-53 Rev. 4 IR-8
		RS.CO-3: Information is shared consistent with response plans	**YES**		· NIST SP 800-53 Rev. 4 CA-2 · NIST SP 800-53 Rev. 4 CA-7 · NIST SP 800-53 Rev. 4 CP-2 · NIST SP 800-53 Rev. 4 IR-4 · NIST SP 800-53 Rev. 4 IR-8 · NIST SP 800-53 Rev. 4 PE-6 · NIST SP 800-53 Rev. 4 RA-5 · NIST SP 800-53 Rev. 4 SI-4
		RS.CO-4: Coordination with stakeholders occurs consistent with response plans	**YES**		· NIST SP 800-53 Rev. 4 CP-2 · NIST SP 800-53 Rev. 4 IR-4 · NIST SP 800-53 Rev. 4 IR-8
		RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	**YES**		· NIST SP 800-53 Rev. 4 PM-15 · NIST SP 800-53 Rev. 4 SI-5
	Analysis (RS.AN): Analysis is conducted to ensure adequate response and support recovery activities.	**RS.AN-1:** Notifications from detection systems are investigated	**YES**		· NIST SP 800-53 Rev. 4 AU-6 · NIST SP 800-53 Rev. 4 CA-7 · NIST SP 800-53 Rev. 4 IR-4 · NIST SP 800-53 Rev. 4 IR-5 · NIST SP 800-53 Rev. 4 PE-6 · NIST SP 800-53 Rev. 4 SI-4
		RS.AN-2: The impact of the incident is understood	**YES**		· NIST SP 800-53 Rev. 4 CP-2 · NIST SP 800-53 Rev. 4 IR-4
		RS.AN-3: Forensics are performed	**YES**		· NIST SP 800-53 Rev. 4 AU-7 · NIST SP 800-53 Rev. 4 IR-4
		RS.AN-4: Incidents are categorized consistent with response plans	**YES**		· NIST SP 800-53 Rev. 4 IR-4 · NIST SP 800-53 Rev. 4 IR-5 · NIST SP 800-53 Rev. 4 IR-8
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.	**RS.MI-1:** Incidents are contained	**YES**		· NIST SP 800-53 Rev. 4 IR-4
		RS.MI-2: Incidents are mitigated	**YES**		· NIST SP 800-53 Rev. 4 IR-4
		RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks	**YES**		· NIST SP 800-53 Rev. 4 CA-7 · NIST SP 800-53 Rev. 4 RA-3 · NIST SP 800-53 Rev. 4 RA-5
	Improvements (RS.IM): Organizational response activities	**RS.IM-1:** Response plans incorporate lessons learned	**YES**		· NIST SP 800-53 Rev. 4 CP-2 · NIST SP 800-53 Rev. 4 IR-4

	are improved by incorporating lessons learned from current and previous detection/response activities.				· NIST SP 800-53 Rev. 4 IR-8
		RS.IM-2: Response strategies are updated	**YES**		· NIST SP 800-53 Rev. 4 CP-2 · NIST SP 800-53 Rev. 4 IR-4 · NIST SP 800-53 Rev. 4 IR-8
RECOVER (RC)	**Recovery Planning (RC.RP):** Recovery processes and procedures are executed and maintained to	**RC.RP-1:** Recovery plan is executed during or after an event	**YES**		· NIST SP 800-53 Rev. 4 CP-10 · NIST SP 800-53 Rev. 4 IR-4 · NIST SP 800-53 Rev. 4 IR-8
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	**RC.IM-1:** Recovery plans incorporate lessons learned	**YES**		· NIST SP 800-53 Rev. 4 CP-2 · NIST SP 800-53 Rev. 4 IR-4 · NIST SP 800-53 Rev. 4 IR-8
		RC.IM-2: Recovery strategies are updated	**YES**		· NIST SP 800-53 Rev. 4 CP-2 · NIST SP 800-53 Rev. 4 IR-4 · NIST SP 800-53 Rev. 4 IR-8
	Communications (RC.CO): Restoration activities are coordinated with internal and external parties, such as	**RC.CO-1:** Public relations are managed	**YES**		
		RC.CO-2: Reputation after an event is repaired	**YES**		
		RC.CO-3: Recovery activities are communicated to internal stakeholders and executive and management teams	**YES**		· NIST SP 800-53 Rev. 4 CP-2 · NIST SP 800-53 Rev. 4 IR-4

Binder1

Final Audit Report 2024-04-10

Created:	2024-04-10
By:	Steven Booth (steven.booth@sllboces.org)
Status:	Signed
Transaction ID:	CBJCHBCAABAA3gxcbWKcUsznZs9t_rNcYnEUav2AIv4I

"Binder1" History

Document created by Steven Booth (steven.booth@sllboces.org)
2024-04-10 - 4:07:12 PM GMT

Document emailed to James Cruikshank (jcruikshank@nncsk12.org) for signature
2024-04-10 - 4:08:56 PM GMT

Email viewed by James Cruikshank (jcruikshank@nncsk12.org)
2024-04-10 - 5:07:15 PM GMT

Document e-signed by James Cruikshank (jcruikshank@nncsk12.org)
Signature Date: 2024-04-10 - 5:07:25 PM GMT - Time Source: server

Agreement completed.
2024-04-10 - 5:07:25 PM GMT