

EXHIBIT A: DATA SHARING AND CONFIDENTIALITY AGREEMENT

Including

**Forestville Central School District Bill of Rights for Data Security and Privacy and
Supplemental Information about a Master Agreement between
Forestville Central School District and Scholastic Inc.**

1. Purpose

(a) **Forestville Central School District** (herein after "District") and Scholastic Inc. inclusive of its affiliates (hereinafter "Vendor" or "Scholastic") are parties to a contract, Terms of Service, or other written agreement pursuant to which Vendor will receive student data and/or teacher or principal data that is protected under New York Education Law Section 2-d and Part 121 of the Regulations of the Commissioner of Education (collectively referred to as "Section 2-d") from the District for purposes of providing certain products or services to the District (the "Master Agreement").

(b) This Exhibit supplements the Master Agreement, to ensure that the Master Agreement conforms to the requirements of Section 2-d. This Exhibit consists of a Data Sharing and Confidentiality Agreement, a copy of the District's Bill of Rights for Data Security and Privacy signed by Vendor, and the Supplemental Information about the Master Agreement between **Forestville Central School District** and **Vendor** that the District is required by Section 2-d to post on its website.

(c) In consideration of the mutual promises set forth in the Master Agreement, Vendor agrees that it will comply with all terms set forth in the Master Agreement and this Exhibit. To the extent that any terms contained in the Master Agreement, or any terms contained in any other Exhibit(s) attached to and made a part of the Master Agreement, conflict with the terms of this Exhibit, the terms of this Exhibit will apply and be given effect. In addition, in the event that Vendor has online or written Privacy Policies or Terms of Service (collectively, "TOS") that would otherwise be applicable to its customers or users of the products or services that are the subject of the Master Agreement between the District and Vendor, to the extent that any terms of the TOS, that are or may be in effect at any time during the term of the Master Agreement, conflict with the terms of this Exhibit, the terms of this Exhibit will apply and be given effect.

2. **Definitions**

As used in this Exhibit:

(a) "Student Data" means personally identifiable information, as defined in Section 2-d, from student records that Vendor may receive from the District pursuant to the Master Agreement.

(b) "Teacher or Principal Data" means personally identifiable information, as defined in Section 2-d, relating to the annual professional performance reviews of classroom teachers or principals that Vendor may receive from the District pursuant to the Master Agreement. District acknowledges that Vendor will not collect any Teacher or Principal Data in connection with the products to which this Agreement applies.

(c) "Protected Data" means Student Data and/or Teacher or Principal Data, to the extent applicable to the product or service actually being provided to the District by Vendor pursuant to the Master Agreement.

(d) "NIST Cybersecurity Framework" means the U.S. Department of Commerce National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1).

3. **Confidentiality of Protected Data**

(a) Vendor acknowledges that the Protected Data it receives pursuant to the Master Agreement originates from the District and that this Protected Data belongs to and is owned by the District.

(b) Vendor will maintain the confidentiality of the Protected Data it receives in accordance with federal and state law (including but not limited to Section 2-d) and the District's policies on data security and privacy. . The District will provide Vendor with a copy of its policy on data security and privacy upon written request.

Confidential information shall not be deemed to include information which:(i) is now or hereafter becomes generally known or available to the public, other than through an act or failure to act on the part of the Vendor; (ii) is known by the Vendor prior to the time of receiving such information; (iii) is hereafter furnished to the Vendor by a third party and to the best of the Vendor's knowledge such third party has no obligation of confidentiality; (iv) is independently developed by the Vendor without any breach of this Agreement; or (v) is the subject of a written permission to disclose provided by the District. For the avoidance of doubt, the foregoing exclusions (i)-(v) shall in no way lessen Vendor's obligations hereunder with respect to data consisting of Protected Data.

4. **Data Security and Privacy Plan**

As more fully described herein, throughout the term of the Master Agreement, Vendor will have a Data Security and Privacy Plan in place to protect the confidentiality, privacy and security of the Protected Data it receives from the District. Vendor's Plan for protecting the District's Protected Data includes, but is not limited to, its agreement to comply with the terms of the District's Bill of Rights for Data Security and Privacy, a copy of which is set forth below and has been signed by the Vendor.

Additional components of Vendor's Data Security and Privacy Plan for protection of the District's Protected Data throughout the term of the Master Agreement are as follows:

(a) Vendor will implement all state, federal, and local data security and privacy requirements including those contained within the Master Agreement and this Data Sharing and Confidentiality Agreement, consistent with the District's data security and privacy policy as provided to the Vendor.

(b) Vendor will have specific administrative, operational and technical safeguards and practices in place to protect Protected Data that it receives from the District under the Master Agreement.

(c) Vendor will comply with all obligations contained within the section set forth in this Exhibit below entitled "Supplemental Information about a Master Agreement between **Forestville Central School District** and **Vendor**". Vendor's obligations described within this section include, but are not limited to:

- i. its obligation to require subcontractors or other authorized persons or entities to whom it may disclose Protected Data (if any) to be subject to confidentiality and data protection obligations imposed on Vendor by state and federal law. Scholastic ensures that its subcontractors will abide by such obligations through a combination of technical due diligence, trainings, contractual obligations, instructions, oversight, audits, and periodic tests, scans and other assessments, as appropriate, and
- ii. its obligation to follow certain procedures for the return, transition, deletion and/or destruction of Protected Data upon termination, expiration or assignment (to the extent authorized in writing by the District to Vendor) of the Master Agreement.

(d) Vendor has provided or will provide training on the federal and state laws governing confidentiality of Protected Data for any of its officers or employees (or officers or employees of any of its assignees) who will have access to Protected Data, prior to their receiving access.

(e) Vendor will manage data security and privacy incidents that implicate Protected Data and will develop and implement plans to identify breaches and unauthorized disclosures. Vendor will provide prompt notification to the District of any breaches or unauthorized disclosures of Protected Data in accordance with the provisions of Section 5 of this Data Sharing and Confidentiality Agreement.

5. **Notification of Breach and Unauthorized Release**

(a) Vendor will promptly notify the District of any breach or unauthorized release of Protected Data it has received from the District in the most expedient way possible and without unreasonable delay, but no more than seven (7) calendar days after Vendor has confirmed the breach or unauthorized release.

(b) Vendor will provide such notification to the District by contacting **Wesley Wright, Director of Technology** directly by email at **wwright@forestville.com** or by calling **716-965-6565**.

(c) Vendor will cooperate with the District and provide as much information as possible directly to **Wesley Wright** or his/her designee about the incident, including but not limited to: a description of the incident, the date of the incident, the date Vendor discovered or was informed of the incident, a description of the types of Protected Data involved, an estimate of the number of records affected, the schools within the District affected, what the Vendor has done or plans to do to investigate the incident, stop the breach and mitigate any further unauthorized access or release of Protected Data, and contact information for Vendor representatives who can assist affected individuals that may have additional questions.

(d) Vendor acknowledges that upon initial notification from Vendor, the District, as the educational agency with which Vendor contracts, has an obligation under Section 2-d to in turn notify the Chief Privacy Officer in the New York State Education Department ("CPO"). Vendor agrees not to provide this notification to the CPO directly unless requested by the District or otherwise required by law. In the event the CPO contacts Vendor directly or requests more information from Vendor regarding the incident after having been initially informed of the incident by the District, Vendor will promptly inform **Wesley Wright** or his/her designee.

(e) Except as otherwise required by law or agreed in writing between the parties and excluding Student Data or any other data that belongs to the District, all information provided by Vendor to the District pursuant to this Agreement shall be treated as Vendor's confidential information. The District agrees that it will disclose such information only to such parties that the District determines are necessary to assist it in its review and require such parties to enter into non-disclosure agreements or otherwise agree in writing to maintain its confidentiality. To the extent permitted by law, the District will withhold such information from public disclosure.

6. **Additional Statutory and Regulatory Obligations**

Vendor acknowledges that it has the following additional obligations under Section 2-d with respect to any Protected Data received from the District, and that any failure to fulfill one or more of these statutory or regulatory obligations will be deemed a breach of the Master Agreement and the terms of this Data Sharing and Confidentiality Agreement:

(a) To limit internal access to Protected Data to only those employees or subcontractors that are determined to have legitimate educational interests within the meaning of Section 2-d and the Family Educational Rights and Privacy Act (FERPA); *i.e.*, they need access in order to assist Vendor in fulfilling one or more of its obligations to the District under the Master Agreement.

(b) To not use Protected Data for any purposes other than those explicitly authorized in this Data Sharing and Confidentiality Agreement and the Master Agreement.

(c) To not disclose any Protected Data to any other party, except for authorized representatives of Vendor using the information to carry out Vendor's obligations to the District and in compliance with state and federal law, regulations and the terms of the Master Agreement, unless:

- (i) the parent or eligible student has provided prior written consent; or
- (ii) the disclosure is required by statute or court order and notice of the disclosure is provided to the District no later than the time of disclosure, unless such notice is expressly prohibited by the statute or court order.

(d) To maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of Protected Data in its custody.

(e) To use encryption technology to protect Protected Data in its custody while in motion or at rest, using a technology or methodology specified by the Secretary of the U.S. Department of Health and Human Services in guidance issued under Section 13402(H)(2) of Public Law 111-5.

(f) To adopt technologies, safeguards and practices that align with the NIST Cybersecurity Framework.

(g) To comply with the District's policy on data security and privacy as provided to Vendor, and NYS Ed Law, Section 2-d and Part

121.

(h) To not sell Protected Data 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) To notify the District, in accordance with the provisions of Section 5 of this Data Sharing and Confidentiality Agreement, of any breach of security resulting in an unauthorized release of Protected Data by Vendor or its assignees or subcontractors as required by applicable state or federal law, the District's Bill of Rights for Data Security and Privacy, the District's policies on data security and privacy, or other binding obligations relating to data privacy and security contained in the Master Agreement and this Exhibit.

(j) To cooperate with the District and law enforcement to protect the integrity of investigations into the breach or unauthorized release of Protected Data.

(k) To pay for or promptly reimburse the District for the full cost of notification, in the event the District is required under Section 2-d to notify affected parents, students, teachers or principals of a breach or unauthorized release of Protected Data attributed to Vendor or its subcontractors or assignees.

FORESTVILLE CENTRAL SCHOOL DISTRICT

PARENTS' BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY

The Forestville School District is committed to protecting the privacy and security of student data and teacher and principal data. In accordance with New York Education Law Section 2-d and its implementing regulations, the District informs the school community of the following:

- 1) A student's personally identifiable information cannot be sold or released for any commercial purposes.
- 2) Parents have the right to inspect and review the complete contents of their child's education record.
- 3) State and federal laws protect the confidentiality of personally identifiable information, and safeguards associated with industry standards and best practices, including but not limited to encryption, firewalls, and password protection, must be in place when data is stored or transferred.
- 4) A complete list of all student data elements collected by New York State is available for public review at the following website <http://www.nysed.gov/student-data-privacy/student-data-inventory> or by writing to the Office of Information and Reporting Services, New York State Education Department, Room 865 EBA, 89 Washington Avenue, Albany, New York 12234.
- 5) Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed in writing to Privacy Complaint, Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, New York 12234. Complaints may also be submitted using the form available at the following website <http://www.nysed.gov/student-data-privacy/form/report-improper-disclosure>.

APPENDIX

Supplemental Information Regarding Third-Party Contractors

In the course of complying with its obligations under the law and providing educational services to District residents, the Forestville School District has entered into agreements with certain third-party contractors. Pursuant to these agreements, third-party contractors may have access to "student data" and/or "teacher or principal data," as those terms are defined by law and regulation.

For each contract or other written agreement that the District enters into with a third-party contractor where the third-party contractor receives student data or teacher or principal data from the District, the following supplemental information will be included with this Bill of Rights:

- 1) The exclusive purposes for which the student data or teacher or principal data will be used by the third-party contractor, as defined in the contract;
- 2) How the third-party contractor will ensure that the subcontractors, or other authorized persons or entities to whom the third-party contractor will disclose the student data or teacher or principal data, if any, will abide by all applicable data protection and security

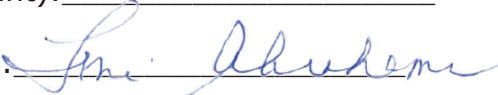
requirements, including but not limited to those outlined in applicable laws and regulations (e.g., FERPA; Education Law Section 2-d);

- 3) The duration of the contract, including the contract's expiration date, and a description of what will happen to the student data or teacher or principal data upon expiration of the contract or other written agreement (e.g., whether, when, and in what format it will be returned to the District, and/or whether, when, and how the data will be destroyed);
- 4) If and how a parent, eligible student, teacher, or principal may challenge the accuracy of the student data or teacher or principal data that is collected;
- 5) Where the student data or teacher or principal data will be stored, described in a manner as to protect data security, and the security protections taken to ensure the data will be protected and data privacy and security risks mitigated; and
- 6) Address how the data will be protected using encryption while in motion and at rest.

Adopted: 12/3/2020

BY THE VENDOR:

Name (Print): Toni Abrahams

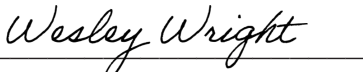
Signature: 

Title: VP of Operations

Date: 1/29/24

BY THE DISTRICT:

Name (Print): Wesley Wright

Signature: 

Title: Director of Technology and Communications

Date: 2/8/2024

Type text here

EXHIBIT B

BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY -

SUPPLEMENTAL INFORMATION FOR CONTRACTS THAT UTILIZE PERSONALLY IDENTIFIABLE INFORMATION

Pursuant to Education Law § 2-d and Section 121.3 of the Commissioner's Regulations, the Educational Agency (EA) is required to post information to its website about its contracts with third-party contractors that will receive Personally Identifiable Information (PII).

Name of Contractor	Scholastic Inc.
Description of the purpose(s) for which Contractor will receive/access PII	Contractor will receive PII data in order to provide all digital education products and Mary Glasgow Learning Magazines ("MGM"). See Contractor's current list of digital education products at: https://educationsolutions.scholastic.com/privacypolicy.html . The privacy policy for MGM can be found at: https://maryglasgowplus.com/privacy .
Type of PII that Contractor will receive/ access	Check all that apply: ☒ Student PII ☐ APPR Data
Contract Term	Contract Start Date <u>Commences as set forth in the applicable ordering document.</u> Contract End Date <u>When subscription ends as set forth in the applicable ordering document, or is terminated.</u>
Subcontractor Written Agreement Requirement	☒ Contractor will not utilize subcontractors¹. ☐ Contractor will utilize subcontractors.
Data Transition and Secure Destruction	Upon expiration or termination of the Contract, and upon written request Contractor shall: • Securely transfer data to EA, or a successor contractor at the EA's option and written discretion, in a format agreed to by the parties. • Securely delete, de-identify, and/or destroy data.

¹ Scholastic may engage some staff on an independent contractor basis, and Scholastic may use third party service providers on an enterprise basis, but Scholastic does not subcontract out any of the services subject to the agreement.

Challenges to Data Accuracy	Parents, teachers or principals who seek to challenge the accuracy of PII will do so by contacting the EA. If a correction to data is deemed necessary, the EA will notify Contractor. Contractor agrees to facilitate such corrections within 30days of receiving the EA's written request.
Secure Storage and Data Security	Please describe where PII will be stored and the protections taken to ensure PII will be protected: (check all that apply) X Using a cloud or infrastructure owned and hosted by a third party. (Amazon Web Services) ☐ Contractor owned and hosted solution. ☐ Other: Please describe how data security and privacy risks will be mitigated in a manner that does not compromise the security of the data: The security protection taken to ensure data will be protected include standards that will align with the NIST cybersecurity framework. Protected data is encrypted in motion (currently with TLS 1.2 128-bit encryption) and at rest (currently with 256 bit AES encryption). Contractor conducts periodic risk assessments and keeps audit trails and security logs to assess and remediate vulnerabilities and to protect data from deterioration or degradation. Additional measures include firewalls, anti-virus and intrusion detection, configuration control and automated backups. Data is classified by sensitivity, and access to data is rule- and role-based.

Encryption	Data will be encrypted while in motion and at rest.
-------------------	--

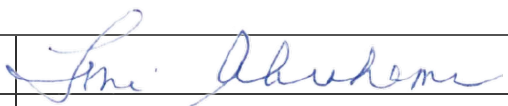
CONTRACTOR	
[Signature]	
[Printed Name]	Toni Abrahams
[Title]	VP of Operations

EXHIBIT C - CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

The Educational Agency (EA) is required to ensure that all contracts with a third-party contractor include a Data Security and Privacy Plan, pursuant to Education Law § 2-d and Section 121.6 of the Commissioner's Regulations. For every contract, the Contractor must complete the following or provide a plan that materially addresses its requirements, including alignment with the NIST Cybersecurity Framework, which is the standard for educational agency data privacy and security policies in New York state. **While this plan is not required to be posted to the EA's website, contractors should nevertheless ensure that they do not include information that could compromise the security of their data and data systems.**

1	Outline how you will implement applicable data security and privacy contract requirements over the life of the Contract.	See Exhibit C.1 Data Security and Privacy Plan.
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	See Exhibit C.1 Data Security and Privacy Plan.
3	Address the training received by your employees or other personnel engaged in the provision of services under the Contract on the federal and state laws that govern the confidentiality of PII.	See Exhibit C.1 Data Security and Privacy Plan.
4	Outline contracting processes that ensure that your employees and any subcontractors are bound to the requirements of the Contract, at a minimum.	See Exhibit C.1 Data Security and Privacy Plan.
5	Specify how you will manage any data security and privacy incidents that implicate PII and describe any specific plans you have in place to identify breaches and/or unauthorized disclosures, and to meet your obligations to report incidents to the EA.	See Exhibit C.1 Data Security and Privacy Plan.
6	Describe how data will be transitioned to the EA when no longer needed by you to meet your contractual obligations, if applicable.	See Exhibit C.1 Data Security and Privacy Plan.
7	Describe your secure destruction practices and how certification will be provided to the EA.	See Exhibit C.1 Data Security and Privacy Plan.
8	Outline how your data security and privacy program/practices align with the EA's applicable policies.	Scholastic's Data Security and Privacy plan covers the elements set forth in the agreement and applicable law, which means our program and practices align.
9	Outline how your data security and privacy program/practices materially align with the NIST CSF v1.1 using the Framework chart below.	See Exhibit C.2 below

Exhibit C.1 SCHOLASTIC INC. DATA SECURITY AND PRIVACY PLAN

In connection with the Data Sharing and Confidentiality Agreement (the “Agreement”) between Scholastic Inc. (“Vendor” or “Scholastic”) and the Forestville Central School District (the “District”), as amended, for the license of certain Scholastic products, Vendor acknowledges that it has read and can comply with the District’s Parents’ Bill of Rights for Data Privacy and Security, the provisions of which are hereby incorporated into this Data Security and Privacy Plan to the extent applicable to Vendor’s use and possession of student data subject to New York Education Law Section 2-d (“Protected Data”). Any capitalized terms not defined herein shall have the meanings given to them in the Agreement.

More specifically, and in furtherance thereof:

1. To implement all applicable data security and privacy requirements (whether by law, contract or policy of the applicable school, district, or other educational agency), Scholastic ensures that relevant staff are advised of data security and confidentiality requirements in district agreements and receive appropriate training (as described further below).
2. Scholastic only uses Protected Data as necessary to provide the licensed educational products and services for the benefit of the District, and access to Protected Data is limited to those employees or sub-contractors who need access for Scholastic to provide such products or services. On expiration of the applicable license agreement and at the District’s written request, Protected Data will be destroyed, returned or de-identified as set forth in the Agreement. The term of the license agreement is as indicated in the agreement, order form or similar document entered into by the parties.
3. Scholastic may retain subcontractors or service providers to assist it in performing services for and providing products to educational agencies. Scholastic does not share Protected Data with third parties other than subcontractors or service providers who are subject to contractual confidentiality and data security obligations, and who may not use the protected data for their own purposes. Scholastic ensures that its personnel, subcontractors and service providers will abide by such obligations through a combination of technical due diligence, trainings, contractual obligations, instructions, oversight, audits, and periodic tests, scans and other assessments.
4. If a parent or eligible student requests to see or challenge the accuracy of any student data, Scholastic’s standard procedure is to refer any such inquires to the participating educational agency and await further instruction. Scholastic will comply with the applicable participating educational agency’s procedure for access to or amendment of education records, subject to applicable law.
5. Scholastic retains data collected through the products for as long as reasonably necessary to provide the product or services and as specified in the applicable contract or otherwise directed by the educational customer.
6. To protect the security, confidentiality and integrity of protected New York state education data, Scholastic will utilize reasonable administrative, technical, operational and physical safeguards and practices including without limitation the following:
 - a. Scholastic stores and processes student data in accordance with industry standards including implementing appropriate administrative, physical and technical safeguards to protect it against unauthorized access, disclosure, alteration and use. Such safeguards align with the NIST Cybersecurity Framework.

- b. Scholastic personnel are required to sign a company confidentiality policy upon hiring, which covers customer information.
 - c. Physical security measures include security personnel and ID-only building access.
 - d. Data is classified by sensitivity, and access to data is rule- and role-based. Internal Vendor personnel access to Protected Data is further protected by multi-factor authentication and VPN requirements.
 - e. With respect to electronic data, no data is stored in “terrestrial” servers.
 - f. Scholastic conducts periodic risk assessments and keeps audit trails and security logs to assess and remediate vulnerabilities and to protect data from deterioration and degradation. Additional measures include firewalls, anti-virus and intrusion detection, configuration control and automated backups. Sensitive data is encrypted in transit (as of the date of the Agreement, with TLS1.2 128-bit encryption) and at rest (as of the date of the Agreement, with 256-bit AES encryption).
 - g. With respect to school users, Scholastic limits unsuccessful logon attempts, enforces minimum password complexity (unless the participating educational agency opts to utilize an “easy log-in” option available in some products for students in K-2 who may have difficulty with traditional log-in, for example pre-literate students, if available in a given product), and employs cryptographic mechanisms to protect the confidentiality of remote access sessions.
7. Without limitation of other training programs that Scholastic may utilize from time to time, Scholastic has provided and will provide the following data security and privacy awareness training to officers and staff with access to Protected Data:
- a. In-person group training sessions on children’s privacy and student privacy, covering applicable laws and best practices.
 - b. Third party online / interactive training sessions on privacy matters and data security available within company intranet and learning resources library.
 - c. Customized/proprietary Scholastic online / interactive training on the Children’s Online Privacy Protection Act available within company intranet and learning resources library.
 - d. In-house written guidelines on children’s privacy compliance available through company intranet.
 - e. Ongoing advice and counsel from in-house and external legal and technical advisors.
8. If Scholastic becomes aware of a security breach that results in the unauthorized release of Protected Data in its possession or control (whether directly or via a subcontractor or third party service provider) in violation of applicable law or contractual obligation, Scholastic will immediately investigate, take steps to mitigate the breach and notify the participating educational agency in the most expedient way possible and without unreasonable delay (no later than 7 calendar days after the discovery of the breach). Scholastic will cooperate with the participating educational agency and law enforcement to protect the integrity of investigations into the breach. If the breach is due to the act

or omission of Scholastic or its subcontractor or service provider, Scholastic will pay or reimburse the participating educational agency for the full cost of legally-required breach notifications.

9. Without limitation of anything contained in the Agreement, when a subscription period for any digital application ends and subject to applicable law and any other specific terms agreed by contract with the school customer, and without limitation of any “self-service” data deletion tools available in the applicable product, Scholastic retains Protected Data collected in connection with the product until the school customer provides written instructions on renewal and/or data disposition. If Scholastic receives no such instructions, student data will be retained and deleted in accordance with Scholastic’s standard data retention and deletion policies.
10. Subject to any other specific terms agreed by contract with the school customer, at any time a customer may request the deletion of Protected Data, which must be provided in writing (mail or email) to Scholastic either through its customer service team or another Scholastic account representative. Scholastic reserves the right to require verification of identity and confirmation of any necessary consents. Once the deletion is complete Scholastic will provide confirmation in writing if required by the customer. Deletion may take the form of overwriting, pseudonymization or irreversible de-identification to the extent permitted by law.

EXHIBIT C.2 – NIST CSF TABLE

The table below will aid the review of a Contractor's Data Privacy and Security Plan. Contractors should complete the Contractor Response sections in the table below to describe how their policies and practices align with each category in the Data Privacy and Security Plan template. To complete these 23 sections, a Contractor may: (i) Demonstrate alignment using the National Cybersecurity Review (NCSR) Maturity Scale of 1-5; (ii) Use a narrative to explain alignment (may reference its applicable policies); and/or (iii) Explain why a certain category may not apply to the transaction contemplated. Further informational references for each category can be found on the NIST website at <https://www.nist.gov/cyberframework/new-framework>. Please use additional pages if needed.

Function	Category	Contractor Response
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 organizational objectives and the organization's risk strategy.	Policy Maturity: 4.5 Practice Maturity: 4.2
	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	Policy Maturity: 4.5 Practice Maturity: 3.5
	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.	Policy maturity: 4.5 Practice Maturity: 4.0
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	Policy Maturity: 4.5 Practice Maturity: 4.2
	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	Policy Maturity: 4.0 Practice Maturity: 4.2
	Supply Chain Risk Management (ID.SC): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.	Policy Maturity: 3.5 Practice Maturity: 3.5

PROJECT (PR)	Identity Management, Authentication and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	Policy Maturity: 4.5 Practice Maturity: 4.0
	Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.	Policy Maturity: 4.5 Practice Maturity: 5.0
	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.	Policy Maturity: 4.5 Practice Maturity: 4.2
	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.	Policy Maturity: 4.5 Practice Maturity: 4.0
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	Policy Maturity: 4.0 Practice Maturity: 4.0
	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.	Policy Maturity: 4.5 Practice Maturity: 4.3

DETECT (DE)	Anomalies and Events (DE.AE): Anomalous activity is detected and the potential impact of events is understood.	Policy Maturity: 4.5 Practice Maturity: 4.5
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	Policy Maturity: 4.5 Practice Maturity: 5.0
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	Policy Maturity: 4.5 Practice Maturity: 5.0
RESPOND (RS)	Response Planning (RS.RP): Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.	Policy Maturity: 4.3 Practice Maturity: 4.4
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	Policy Maturity: 4.3 Practice Maturity: 4.5
	Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.	Policy Maturity: 4.3 Practice Maturity: 5.0
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	Policy Maturity: 4.3 Practice Maturity: 4.5
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	Policy Maturity: 4.3 Practice Maturity: 4.5
RECOVER (RC)	Recovery Planning (RC.RP): Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.	Policy Maturity: 4.0 Practice Maturity: 4.0
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	Policy Maturity: 4.0 Practice Maturity: 4.0

	Communications (RC.CO): Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).	Policy Maturity: 4.0 Practice Maturity: 4.0
--	--	--

