Supplemental Agreement between the

Hewlett-Woodmere Union Free School District

And

New York Therapy Placement Services Inc.

Supplemental Agreement dated this 1st day of July 2023 between the Hewlett-Woodmere Union Free School District (the "District"), located at One Johnson Place, Woodmere, NY 11598, and **New York Therapy Placement Services Inc.**

(the "Contractor") located at 299 Hallock Avenue, Port Jefferson Station, NY 11776

WHEREAS, the District and Contractor have entered into a contract or other written agreement (hereinafter the "Agreement") whereby the Contractor may receive Student Data or Teacher or Principal Data, as those terms are defined in Education Law §2-d and 8 NYCRR 121.1; and

WHEREAS, the District and Contractor wish to enter into an agreement in order to comply with Education Law §2-d and 8 NYCRR Part 121 (hereinafter "Supplemental Agreement").

NOW THEREFORE, in consideration of the mutual promises below, the District and Contractor agree as follows:

1. Defined Terms: Unless otherwise indicated below or elsewhere in this Supplemental Agreement, all capitalized terms shall have the meanings provided in Education Law §2-d and Section 121.1 of the Regulations of the Commissioner of Education (hereinafter "Regulations").

a. "Educational Agency" shall generally have the same meaning as the term Educational Agency at Education Law §2-d(1)(c) and Section 121.1(f), and in reference to the party to this Agreement shall mean the Hewlett-Woodmere Union Free School District.

b. "Third Party Contractor" shall mean any person or entity, other than an Educational Agency, that receives Student Data or Teacher or Principal Data from an Educational Agency pursuant to a contract or other written agreement for purposes of providing services to such Educational Agency, including but not limited to data management or storage services, conducting studies for or on behalf of such Educational Agency, or audit or evaluation of publicly funded programs. With reference to this agreement, "Third Party Contractor" shall be synonymous with "Contractor" and shall also include any and all subcontractors, persons or entities with whom the Contractor shares Student Data and/or Principal or Teacher Data pursuant to a contract or other written agreement for purposes of providing services to such Educational Agency, including but not limited to data management or storage services, conducting studies for or on behalf of such Educational Agency, or audit or evaluation of publicly funded programs.

c. "Student" means any person attending or seeking to enroll in an Educational Agency.

d. "Student Data" means Personally Identifiable Information of a "Student."

e. "Eligible Student" means a Student who is eighteen years or older.

f. "Parent" means a parent, legal guardian, or personal in parental relation to a Student.

g. "Building Principal" or "Principal" means a building principal subject to annual performance evaluation review under Education Law §3012-c.

h. "Classroom Teacher" or "Teacher" means a teacher subject to annual performance evaluation review under Education Law §3012-c.

i. "Teacher or Principal Data" means Personally Identifiable Information from the records of an Educational Agency relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of Education Law §3012-c.

j. "Personally Identifiable Information" shall have the following meanings:

i. As applied to Student Data, shall mean Personally Identifiable Information as defined in 34 CFR 99.3 implementing the Family Educational Rights and Privacy Act (FERPA)

ii. As applied to Teacher or Principal Data, shall mean Personally Identifiable Information as that term is defined in Education Law §3012-c.

2. The District has developed the Parents Bill of Rights for Data Privacy and Security, the terms of which are applicable to the Agreement between the District and Contractor and are incorporated into this Supplemental Agreement. The Parents Bill of Rights for Data Privacy and Security states:

Pursuant to New York State Education Law §2-d, parents, legal guardians and persons in parental relation to a student are entitled to certain rights with regard to their child's personally identifiable information, as defined by Education Law §2-d. The Hewlett-Woodmere Public School District, in recognition of the risk of identity theft and unwarranted invasion of privacy, affirms its commitment to safeguarding student personally identifiable information (PII) in educational records from unauthorized access or disclosure in accordance with State and Federal law. This document contains a plain-English summary of such rights.

1. Student PII will be collected and disclosed only as necessary to achieve educational purposes in accordance with State and Federal Law.

2. A student's personally identifiable information cannot be sold or released for any commercial or marketing purposes by the District or any a third party contractor. The district will not sell student personally identifiable information and will not release it for marketing or commercial purposes, other than directory information released by the district in accordance with district policy;

3. Parents have the right to inspect and review the complete contents of their child's educational records maintained by the Hewlett-Woodmere Public Schools. (for more information about how to exercise this right, see 5500-R);

4. State and Federal Laws, such as NYS Education Law §2-d and the Family Educational Rights and Privacy Act, protect the confidentiality of students' personally identifiable student information. 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;

5. A complete list of all student data elements collected by New York State is available for review at the following website:

    a. http://www.p12.nysed.gov/irs/sirs/documentation/NYSEDstudentData.xlsx

6. The list may also be made available by writing to:

    Chief Privacy Officer
    New York State Education Department
    89 Washington Avenue
    Albany, NY 12234

7. Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed to:

    Assistant Superintendent for Teaching, Learning, and Technology
    Hewlett-Woodmere Public Schools
    1 Johnson Place
    Woodmere, New York 11598
    (516) 792-4802

    OR

    Complaints can also be directed to the New York State Education Department online at http://nysed.gov.data-privacy-security, by mail to the

    Chief Privacy Officer
    New York State Education Department
    89 Washington Avenue
    Albany, NY 12234

    Email: privacy@mail.nysed.gov

Telephone at 518-474-0937

8. Parents have the right to be notified in accordance to applicable laws and regulations if a breach or unauthorized release of their student's PII occurs.

9. Parents can expect that educational agency workers who handle PII will receive annual training on applicable federal and state laws, regulations, educational agency's policies and safeguards which will be in alignment with industry standards and best practices to protect PII.

10. In the event that the District engages a third-party provider to deliver student educational services, the contractor or subcontractor will be obligated to adhere to State and Federal Laws to safeguard student PII. Parents can request information about third party contractors by contacting

    Amanda Kavanagh
    Data Protection Officer
    Hewlett-Woodmere Public Schools
    1 Johnson Place
    Woodmere, New York 11598
    (516) 792-4892
    akavanagh@hewlett-woodmere.net

    or can access the information on the District's website:
    https://www.hewlett-woodmere.net/Page/11125

Each contract with a third-party contractor which will receive student data, or teacher or principal data will include information addressing the following:

a. The exclusive purposes for which the student data or teacher or principal data will be used.

b. How the third-party contractor will ensure that the subcontractors, persons or entities that the third-party contractor will share the student data or teacher or principal data with, if any, will abide by data protection and security requirements.

c. When the agreement expires and what happens to the student data or teacher and principal data upon expiration of the agreement.

d. If and how a parent, student, a student over eighteen years of age, teacher or principal may challenge the accuracy of the student data or teacher or principal data that is collected; and

e. Where the student data or teacher or principal data will be stored, and the security protections taken to ensure such data will be protected, including whether such data will be encrypted.

7. Third-party contractors are also required to:

   a. Provide training on federal and state law governing confidentiality to any officers, employees, or assignees who have access to student data or teacher or principal data;

   b. Limit internal access to education records to those individuals who have a legitimate educational interest in such records.

   c. Not use educational records for any other purpose than those explicitly authorized in the contract;

   d. Not disclose personally identifiable information to any other party (i) without the prior written consent of the parent or eligible student; or (ii) unless required by statute or court order and the third-party contractor provides a notice of the disclosure to the New York State Education Department, board of education, or institution that provided the information no later than the time the information is disclosed, unless providing notice of the disclosure is expressly prohibited by the statute or court order;

   e. Maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of personally identifiable student information in its custody;

   f. Use encryption technology to protect data while in motion or in its custody from unauthorized disclosure as specified in Education Law §2-d;

   g. Notify the Hewlett-Woodmere Public Schools of any breach of security resulting in an unauthorized release of student data or teacher or principal data, in the most expedient way possible and without unreasonable delay;

   h. Provide a data security and privacy plan outlining how all state, federal and local data security and privacy contract requirements will be implemented over the life of the contract;

   i. Provide a signed copy of this Bill of Rights to the Hewlett-Woodmere Public Schools thereby acknowledging that they are aware of and agree to abide by this Bill of Rights.

8. This Bill of Rights is subject to change based on regulations of the Commissioner of Education and the New York State Education Department's Chief Privacy Officer, as well as emerging guidance documents.

3. As required by Education Law §2-d(3)(c) and Section 121.3 of the Regulations, the Contractor shall comply with the Data Security and Privacy Plan which is attached to this Agreement.

4. As required by Education Law §2-d(5)(e), the Contractor hereby agrees that any officers or employees of the Contractor, including any subcontractors or assignees, who have access to Student Data or Teacher or Principal Data will have or will receive training on the Federal and

New York State laws governing confidentiality of Student Data and/or Principal or Teacher Data prior to receiving access.

5. As required by Education Law §2-d(5)(f), the Contractor hereby agrees that it shall:

a. Limit internal access to education records to those individuals that are determined to have legitimate educational interests;

b. Not use the educational records for any other purposes than those explicitly authorized in the Agreement or this Supplemental Agreement;

c. Except for authorized representatives of the Contractor to the extent they are carrying out the Agreement or this Supplemental Agreement, not disclose any Personally Identifiable Information to any other party:

i. Without the prior written consent of the Parent or Eligible Student; or

ii. Unless required by statute or court order and the party provides a notice of the disclosure to the State Education Department, District Board of Education, or institution that provided the information no later than the time the information is disclosed, unless providing notice of the disclosure is expressly prohibited by the statute or court order.

d. maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of personally identifiable student information in its custody;

6. Breach and unauthorized release of Personally Identifiable Information:

a. In accordance with Education Law §2-d(6) and Section 121.11 of the Regulations, the Contractor shall be required to notify the District of any breach of security resulting in an unauthorized release of Student Data and/or Principal or Teacher Data by the Contractor or its subcontractors or assignees in violation of applicable state or federal law, the Parents Bill of Rights for Student Data Privacy and Security, the data privacy and security policies of the District and/or binding contractual obligations relating to data privacy and security, in the most expedient way possible and without unreasonable delay. The District shall, upon notification by the Contractor, be required to report to the Chief Privacy Officer, who is appointed by the State Education Department, any such breach of security and unauthorized release of such data.

b. In the case of an unauthorized release of Student Data, the District shall notify the Parent or Eligible Student of the unauthorized release of Student Data that includes Personally Identifiable Information from the student records of such Student in the most expedient way possible and without unreasonable delay. In the case of an unauthorized

release of Teacher or Principal Data, the District shall notify each affected Teacher or Principal of the unauthorized release of data that includes Personally Identifiable Information from the Teacher or Principal's annual professional performance review in the most expedient way possible and without unreasonable delay.

c. In the case of notification to a Parent, Eligible Student, Teacher or Principal due to the unauthorized release of student data by the Contractor, or its subcontractors or assignees, the Contractor shall promptly reimburse the educational agency for the full cost of such notification, as required by Education Law §2-d(6)(c).

7. Miscellaneous:

a. The District and Contractor agree that if applicable laws change and/or if the Commissioner of Education implements Regulations which affects the obligations of the parties herein, this Agreement shall be deemed to incorporate such changes as necessary in order for the District and the Contractor to operate in compliance with the amendment or modified requirements under the applicable laws or regulations.

b. Any ambiguity in this Agreement shall be resolved in favor of a meaning that permits the District to comply with the applicable laws or regulations.

c. Nothing express or implied in this Agreement is intended to confer upon any person other than the District, Contractor and their respective successors and assigns any rights, remedies, obligations or liabilities.

d. To the extent that any terms contained within the Contractor's terms of service, privacy policy, other policy or items similar to the foregoing conflict with the terms of this Agreement, the terms of this Agreement shall govern, supersede, and take precedence over any such conflicting terms.

IN WITNESS WHEREOF, the Parties hereto have duly executed this Agreement.

NY Therapy Placement Services Inc.

By: John F. Johnson

Print Name: John F. Johnson

Title: Director of Operations

Date: 6/1/2023

HEWLETT-WOODMERE UNION FREE SCHOOL DISTRICT

By: Marie Donnelly

Print Name: Marie Donnelly

Title: Assistant Superintendent for Finance and Personnel

Date: 9/11/2023

Data Security and Privacy Plan

As per Section 3 of the Supplemental Agreement, this plan must be completed by the Contractor.

1. Exclusive Purposes for Data Use
   a. The exclusive purposes for which the Student Data and/or Principal or Teacher Data will be used by the Contractor are as follows

See attached NYTPS Data Privacy Agreement and Parents' Bill of Rights Supplemental Information Document

Initial JFB

2. Data Accuracy/Correction Practices
   a. Parent, student, eligible student, teacher or principal may challenge the accuracy of the data by

See attached NYTPS Data Privacy Agreement and Parents' Bill of Rights Supplemental Information Document

Initial JFB

3. Security Practices
   a. The security protection taken to ensure data will be protected include [*Insert (i) a description of where Student Data and/or Principal or Teacher Data will be stored, described in a manner to protect data security, (ii) a description of the security protections taken to ensure Student Data and/or Principal or Teacher Data will be protected and data security and privacy risks are mitigated; and (iii) a description of how the Student Data and/or Principal or Teacher Data will be protected using encryption while in motion and at rest.*

See attached NYTPS Data Privacy Agreement and Parents' Bill of Rights Supplemental Information Document

Initial JFB

4. Contract Lifecycle Practices
   a. The agreement expires 6/30/2024
   b. When the agreement expires, the Student Data and/or Principal or Teacher Data will be

See attached NYTPS Data Privacy Agreement and Parents' Bill of Rights Supplemental Information Document

Initial JFJ

5. The Contractor will ensure that any and all subcontractors, persons or entities that the Contractor may share the Student Data and/or Principal or Teacher Data with will abide by the terms of the Agreement, the Supplemental Agreement, and the data protection and security requirements set forth in this Data Security and Privacy Plan, in accordance Education Law §2-d and Part 121 of the Regulations.

Initial JFJ

New York Therapy Placement Services, Inc.

Company Name

John F. Johnson
Director of Operations

Print Name and Title

John F. Johnson 6/1/2023

Signature of Provider Date

Return to:
Amanda Kavanagh
Assistant Superintendent for Teaching, Learning, and Technology
Hewlett-Woodmere Public Schools
1 Johnson Place
Woodmere, NY 11598
akavanagh@hewlett-woodmere.net

New York Therapy Placement Services, Inc.

Serving Infants through Adults • Nassau-Suffolk-NYC

Occupational • Physical • Speech Therapy • Psychology • Special Education
Applied Behavioral Analysis (ABA)

NEW YORK THERAPY PLACEMENT SERVICES, INC.
DATA PRIVACY AGREEMENT AND
PARENTS' BILL OF RIGHTS SUPPLEMENTAL INFORMATION
(FOR RELATED SERVICES CONTRACTS)
Updated: 3/31/22

1. The exclusive purposes for which the student data will be used:

Student data will be used for providing related services to the student.

Access to Child Record Files

Internal employees who have a need to access child records to perform their job duties are given password protected access to the data servers.

Any field employees requiring access to electronic child record files must be pre-authorized to be on our network. The network requires a two-step login process in which the user first must log in to our Virtual Private Network (VPN). Once accepted by the VPN, users then log in again to access the network.

Both internal and field users on the network are required to change passwords every 90 days, and past passwords may not be repeated.

2. Data Accuracy/Correction Practices: How a parent or student may challenge the accuracy of the student data that is collected:

If a parent or eligible student feels the education records relating to the student contain information that is inaccurate, misleading, or in violation of the student's rights of privacy, he or she may ask the agency to amend the record. (FERPA Subpart C, Section 99.20). Parents may exercise their right to request an amendment of their child's educational records by sending their request to:

New York Therapy Placement Services, Inc.
299 Hallock Avenue
Port Jefferson Station, NY 11776
Attn: John Johnson, Director of Operations and Compliance Officer

Phone: 631-473-4284
E-mail: john.johnson@nytps.com

New York Therapy will review the request within a reasonable time of receiving it and notify the requester of its decision to amend the record or not. If the request is denied, the requester has the right to request a hearing to challenge the decision not to amend the records. If after the hearing the agency still maintains that the contents of the record are correct, the requester may place a statement into the record commenting on the contested information or stating why he or she disagrees with the decision of the agency. This statement will be maintained by the agency with the contested part of the record and will be disclosed whenever the agency discloses that portion of the record to which the statement relates.

3. <u>Subcontractor Oversight Details:</u> How the contractor will ensure that subcontractors, persons, or entities with whom it shares student data will abide by data protection and security requirements:

All subcontractors and independent contractors are expected to maintain the same vigilance in protecting personally identifiable information as does the Agency. All subcontractors must sign the New York Therapy Placement Services, Inc. Business Associate Agreement which outlines the following responsibilities pertaining to safeguarding PII:

- *PII will not be disclosed or discussed with others, including friends or family, who do not have a need to know it.*
- *PII will be used, disclosed, accessed, or viewed only to the extent required to carry out responsibilities, except as may be required by law.*
- *PII will not be discussed where others can overhear the conversation. It is not acceptable to discuss PII in public areas even if a patient's name is not used.*
- *Inquiries about PII will not be made on behalf of personnel not authorized to access or view such information.*
- *Safeguards will be established to prevent misuse as well as inappropriate access, alteration, destruction, or disclosure of PII.*
- *Violations of any of the proceeding requirements will be immediately reported to New York Therapy Placement Services, Inc. at 631-473-4284.*
- *After termination or expiration of providers' agreement with New York Therapy Placement Services, Inc., provider remains responsible to continue safeguarding PII.*

4. Data Security and Encryption Practices – NYTPS Hosted Network System

Summary

- **All Servers are Encrypted at the Storage level – while at rest, via VMware Encryption protocols.**

- **All Server Communication is Encrypted at the network level – while in transit, via VMware Encryption protocols.**
- **All Communication is Encrypted at the client connection level – while in transit, via OpenVPN Encryption protocols**

Data Encryption Standards

All hosted servers for NYTPS are housed on a fully redundant, high availability VMware based server and storage system. The VMWare 7.x system includes vSphere Virtual Machine Encryption that supports encryption of virtual machine files, virtual disk files, and core dump files.

Two types of keys are used for encryption:

1. The ESXi host generates and uses internal keys to encrypt virtual machines and disks. These keys are used as data encryption keys (DEKs) and are XTS-AES-256 keys.
2. vCenter Server requests keys from the KMS. These keys are used as the key encryption key (KEK) and are AES-256 keys. vCenter Server stores only the ID of each KEK, but not the key itself.

ESXi uses the KEK to encrypt the internal keys and stores the encrypted internal key on disk. ESXi does not store the KEK on disk. If a host reboots, vCenter Server requests the KEK with the corresponding ID from the KMS and makes it available to ESXi. ESXi can then decrypt the internal keys as needed.

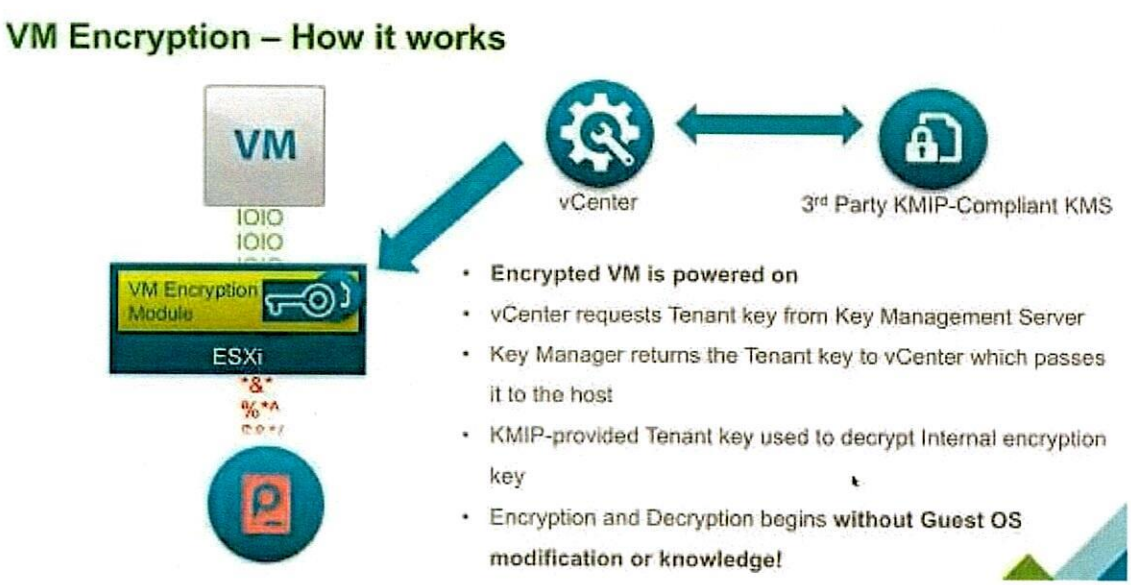
Servers are all encrypted using these standards at the VM level. These servers include the Database server, the file server, and the terminal servers where people remotely login to the box. All data transfers in this encrypted envelope.

All Servers systems (Database, File Storage, Remote Desktop) are contained in a fully encrypted environment using VMware 7.x. All communications between these services happens via either the internal encrypted network in the host sessions or though the client VPN (See Below).

Client Encryption

All clients connect to the remote server environment via a VPN client that supports AES-256-GCM (OpenVPN 2.4+) standards. In additional All computing sessions transfer RDP protocols which have their encryption using TLS MS standards. *All data is encrypted entering/leaving the datacenter via this VPN tunnel.*

The Picture Below Shows how the Server Encryption happens at startup and at rest.



5. <u>Contract Lifecycle Practices</u>: When the agreement expires, what happens to the student data?

Pursuant to The New York State Retention and Disposition Schedule for New York Government Records (LGS-1), New York Therapy Placement Services will retain student data for 6 years after the date of the student's graduation, or 6 years past the child's 21st birthday, whichever is shorter. With written request from the district, NYTPS will destroy student data after that mandated period expires or return the data to the district. NYTPS will provide written certification of the secure deletion and/or destruction of PII. The security measures in this agreement are for the life of the contract, including any extensions, and NYTPS will follow all State, Federal, and local data security and privacy requirements including, without limitation, the District's policy.

6. Where the student data will be stored and the security protections taken to ensure such data will be protected, including whether such data will be encrypted:

The NYTPS network system uses a domain-based Microsoft network. All data is stored on either a file server or database server. Each user has a unique ID and password. Passwords are set to be changed every 90 days for network access. Access to our member database is controlled by additional separate login ID.

All access to the network and database is based on role level access. User accounts are defined by job function and access to network resources are given based on that role. All network accounts are reviewed on at least an annual basis.

Emails that have personally identifiable information (PII) are encrypted using a software system for all outbound emails. Inbound emails can also use this system.

Backups are stored on an in-house system using data password encryption on the drives. Backups are stored in an alternate office location. Windows Systems are updated with all security patches on a bi-weekly basis. Application updates are applied by vendor standards. All desktops and servers have anti-virus applications that update on a daily basis. Server systems have MSBPA (Microsoft Best Practice Analyzer) run on them before going into production and at least annually thereafter.

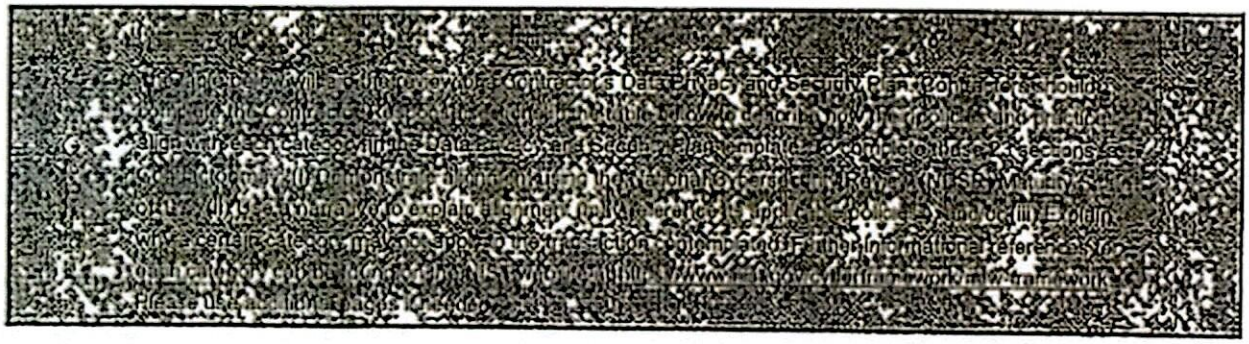
Remote access to network is accessed via a VPN based solution. Only users with a job role need have access to data remotely.

7. NIST Framework – New York Therapy follows the voluntary standards and guidelines of the NIST Framework Version 1.1 to help manage its cybersecurity risk. Please see the following pages for our NIST checklist.

8. Data Privacy Training – All employee staff and officers are provided with privacy training upon joining the company. The company's employee manual contains sections on confidentiality and PII as in accordance with Federal, State, and local law, policy, and regulation including, without limitation, FERPA, NY Education Law Section 2-d, and District policy. Each employee must read the manual and sign an attestation agreeing to the terms of the manual. Similarly, each independent contractor must read and agree to our Business Associate agreement which requires the independent contractor to understand and abide by the aforementioned applicable data protection and security requirements set forth in Federal, State, and local law, policy, and regulation.

9. Breach of Data Security – In the event of the unauthorized acquisition, access, use, or disclosure of Personally Identifiable Information in a manner not permitted by State and federal laws, rules, and regulations or in a manner which compromises its security or privacy, or by or to a person not authorized to acquire, access, use, or receive it, New York Therapy will notify the Educational Agency of the breach without unreasonable delay no later than seven (7) business days after discovery of the breach. Such notification will include, but not be limited to, a description of the breach including the date of the incident and date of discovery, the types of PII affected and the number of records affected; a description of the NYTPS investigation into the breach, and the contact information of NYTPS employees to contact regarding the breach. NYTPS will cooperate with the EA and law enforcement, if necessary, in any investigations into the breach.

EXHIBIT: NIST CSF TABLE



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.	NCSR Level 6
	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	NCSR Level 6
	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.	NCSR Level 6
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	NCSR Level 5
	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	NCSR Level 6

PROJECT (PR)	**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	NCSR Level 6
	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	NCSR Level 6
	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	NCSR Level 4
	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.	NCSR Level 5
	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.	NCSR Level 5
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures	NCSR Level 6
	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.	NCSR Level 6
[illegible]	**Anomalies and Events (DE.AE):**	

DETECT (DE)	Anomalous activity is detected and the potential impact of events is understood.	NCSR Level 6
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	NCSR Level 6
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	NCSR Level 6
RESPOND (RS)	**Response Planning (RS.RP):** Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents	NCSR Level 6
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	NCSR Level 6
	Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.	NCSR Level 5
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	NCSR Level 5
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	NCSR Level 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.	NCSR Level 6
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	NCSR Level 6
	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).	NCSR Level 6