NEW YORK THERAPY PLACEMENT SERVICES, INC.
DATA PRIVACY AND SECURITY PLAN
Updated: 9/29/23

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

All independent contractors are expected to maintain the same vigilance in protecting personally identifiable information as does the Agency. All Independent Contractors 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.

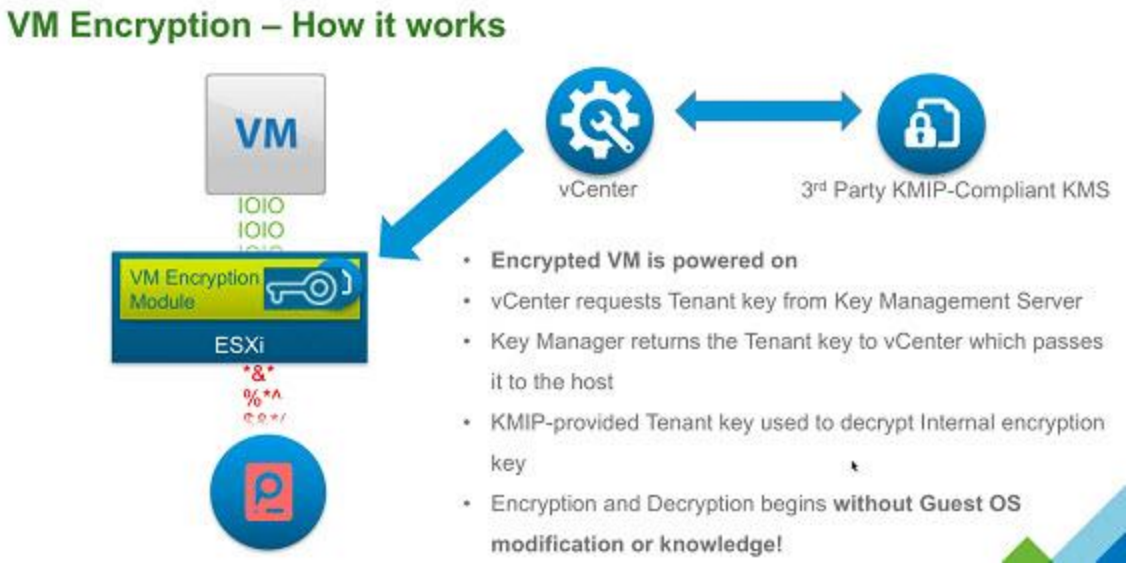
Servers are all encrypted using these standards at the VM level. These servers include the Database server, the file server, and the terminal servers where people remotely login to the box. All data transfers in this encrypted envelope.

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 or as otherwise required by law. 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.

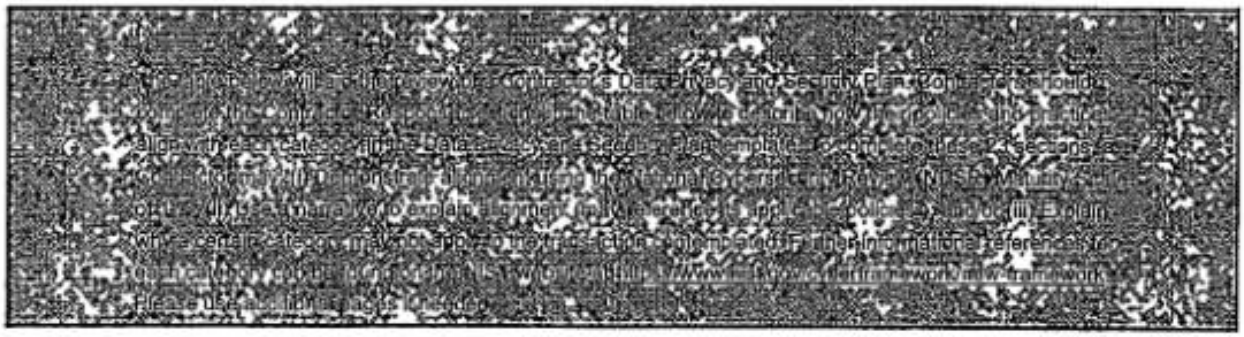
7. NIST Framework – New York Therapy follows the voluntary standards and guidelines of the NIST Framework Version 1.1 to help manage its cybersecurity risk. Please see the following pages for our NIST checklist.

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.

10. Data Security and Privacy Over the Lifetime of the Contract - Contractor will implement applicable state, federal, and local data security and privacy contract requirements over the life of the Contract and only use PII in accordance with the Contract, and applicable laws pertaining to data privacy and security including Education Law § 2-d.

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
[redacted]	**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 activites.	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