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 AND SECURITY PLAN
Updated: 04/10/2024

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

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

Use and Access to Child Record Files

Employees and providers working in the field will have access to Personally Identifiable Information (PII) that is provided by the Local Educational Agency (LEA) or is created in the course of delivering services and will be used only to the extent needed to carry out the special educational services, in accordance with state and federal law and/or contract with the school district.

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. Parents' Bill of Rights and Data Accuracy/Correction Practices: How a parent or student may inspect, review and/or challenge the accuracy of the student data that is collected:

This Data Privacy and Security Plan describes the administrative and technical security measures taken by the agency to safeguard students' personally identifiable information when it is stored or transferred. The plan describes the notification procedures the agency will follow if a breach or unauthorized release of PII occurs. This plan also includes information about how a parent/guardian can request a review and/or amendment to their child's records.

A request from a parent or eligible student to amend, inspect, obtain copies of, or otherwise access student data may be received by New York Therapy, or the LEA. New York Therapy will facilitate and assist the LEA in processing such requests in a timely manner, in accordance with procedure prescribed by the LEA. If a parent or eligible student feels the education record relating to the student held by New York Therapy contains information that is inaccurate, misleading, or in violation of the student's privacy rights, he or she may submit a request to the LEA. If a correction to the information is deemed necessary by the LEA, New York Therapy shall amend the records at the LEA's decision and direction. New York Therapy agrees to facilitate such corrections upon the written request of the LEA. If the LEA decides not to amend the record as requested by the parent or eligible student, he or she will be notified by the LEA of the decision and of their right to a hearing regarding the request for amendment.

New York Therapy will facilitate and comply with all requirements of the Parents' Bill of Rights under NYS Education Law 2-d, which is accessible on our company website, and that of the LEAs with which we conduct business, which can be found on the individual districts' websites.

3. Independent Contractor Oversight Details: 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:

New York Therapy does not subcontract your contract to other agencies. All independent contractors who have access to PII to provide services to students are expected to maintain the same vigilance in protecting personally identifiable information as the Agency's employees. Independent contractors are required by written agreement to abide by materially similar confidentiality and data protection obligations imposed on New York Therapy under state and federal laws and regulations, and the contract with the LEA. All independent contractors are required to complete NYTPS' online Data Privacy and Security Training upon engagement and periodically thereafter. This training reviews data protection and security requirements under state and federal laws governing confidentiality of student data, and the information contained in this Plan. All independent contractors must also sign the New York Therapy Placement Services, Inc. Business Associate Agreement and Corporate Compliance Plan which outline the following responsibilities pertaining to safeguarding PII and/or PHI:

- *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 unauthorized use, 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.

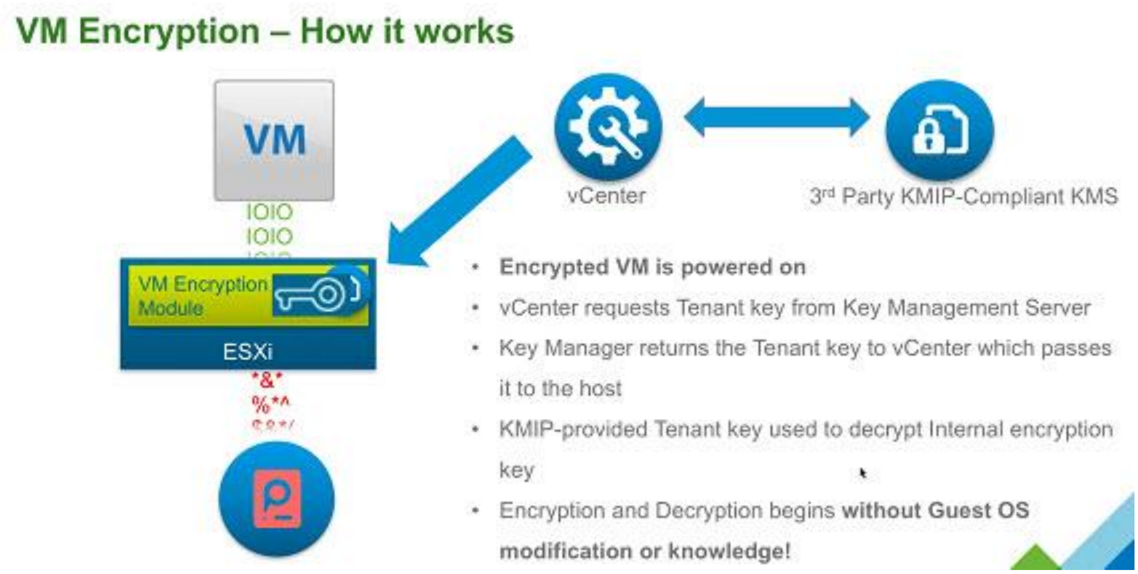
Servers are all encrypted using these standards at the VM level. These servers include the Database server, the file server, and the terminal servers where people remotely login to the box. All data transfers in this encrypted envelope.

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.



VM Encryption – How it works

- **Encrypted VM is powered on**
- vCenter requests Tenant key from Key Management Server
- Key Manager returns the Tenant key to vCenter which passes it to the host
- KMIP-provided Tenant key used to decrypt Internal encryption key
- Encryption and Decryption begins **without Guest OS modification or knowledge!**

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

Except as prescribed by a contract with the LEA or as required by law, upon expiration or termination of the contract with the LEA or after the required retention period, New York Therapy will securely delete/destroy or return data to the LEA (or a successor provider at the LEA's option and written discretion). New York Therapy will follow all state, federal and contractual requirements for the retention, deletion, or destruction of PII and special education records. 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 protected by firewall security measures. All data is stored on either a file server or database server with Active Directory, to authenticate and authorize users and manage all security-related aspects of the domain. Each user has a unique ID and password. Passwords follow NIST guidelines for strong passwords and are set to be changed every 90 days for network access. Access to our member database is controlled by an 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 and deactivated upon employee termination.

NYTPS policy requires that all emails containing personally identifiable information (PII) must be encrypted using established Microsoft 365 encryption protocol.

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. All computer devices run Microsoft 365 Office applications with multi-factor authentication. Application updates are applied by vendor standards. All desktops and servers have anti-virus (MDR) and Endpoint Detection and Response (EDR) that update centrally 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 the network is accessed via a VPN based solution. Only users with a job role need are granted 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 NYTPS' online Data Privacy and Security training upon joining the company and annually thereafter; all independent contractors are provided with the online training upon engagement with the company and periodically thereafter. This training reviews data protection and security requirements under state and federal laws governing confidentiality of student data. The company's employee manual and Corporate Compliance Plan contain sections on confidentiality and PII 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 compliance plan, and sign attestations agreeing to their terms. Similarly, each independent contractor must read and agree to our Business Associate agreement and Corporate Compliance Plan, which require 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.

To meet the training requirements of individual LEAs with which the agency conducts business, the agency may link the data privacy and security policies of the LEA at the end of this document, to be referenced by affected agency staff and/or parents. As an example, the data privacy and security policies of the New York City Department of Education are linked at the end of this document.

9. Data System Monitoring - NYTPS proactively reduces the attack surface by identifying and controlling rogue devices and applications based on risk mitigation policies. We utilize both endpoint detection and response (EDR) and managed detection and response (MDR) technologies to be better prepared and informed. These tools provide details for any issue on every PC and server in the NYTPS environment in real time. Alerts are generated in real-time, and all activity is logged. Additionally, Office 365 provides 90 days of audit logs for every user.

Our MDR is a comprehensive managed security operations solution that protects organizations against threats by using security experts, advanced tools, and threat intelligence. Key benefits include:

- 24/7 environment monitoring
- Threat investigation
- Expert human and automated response
- Expert-managed security operations

Our EDR solutions continuously monitor endpoints for threats, generate alerts when any suspicious activity is detected, enhance the investigation, and provide the ability to respond to and contain potential attacks. Key capabilities of endpoint detection and response include:

- Detection
- Containment
- Investigation
- Eradication

Our Endpoint Protection prevents malware infection and detects potential threats in real-time, even on compromised devices. This tool instantly stops breaches to prevent data loss and ransomware damage with no dwell time.

10. Breach of Data Security/Incident Response – 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 and no later than seven (7) business days after confirmation of a reportable event/breach where PII has been accessed. New York Therapy will comply with any individual LEA's requirement for breach notification which may be shorter. As an example, the agency will comply with the NYC DOE requirement to provide notification within 24 hours of confirmation of a reportable event/breach where PII has been accessed. 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, 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 LEA and law enforcement, if necessary, in any investigations into the breach and will assist and collaborate with the LEA, as requested.

In the event of a breach, NYTPS blocks the suspected user account from the ability to sign into our network and their Office 365 account. The password for the user(s) account(s) will be reset using MFA. The suspected computer or computers are removed from the Active Directory. On site computers are removed from the local network and VPN access for computers off site are disabled. The IT department will run all necessary reports on our network and on our Office 365 account to determine if any student PII on our environment or on the user(s) Office 365 account has been breached. The affected computer(s) are removed from the environment.

The user or users involved in a breach will be required to attend additional Cyber Security training. The user will also be subject to additional internal phishing campaigns to improve awareness and detection.

11. Data Security and Privacy Over the Lifetime of the Contract – NYTPS has implemented administrative and technical safeguards, as described in this Plan, to implement all state, federal, local and contract requirements pertaining to data security and privacy. These measures include monitoring regulatory changes to stay up to date on privacy and security requirements, training of all staff, as well as multi-layered electronic, cyber-security and physical security standards to control, limit and protect the access, storage, use, transmission, and disclosure of confidential information. NYTPS 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.

This Data Privacy and Security Plan is posted on the agency's website, www.nytps.com, and will be updated whenever changes are made. Employees, contractors, and parents may review the plan by clicking the link on the website.

Important Links:

NYSED Parents' Bill of Rights: https://www.nysed.gov/data-privacy-security/bill-rights-data-privacy-and-security-parents-bill-rights

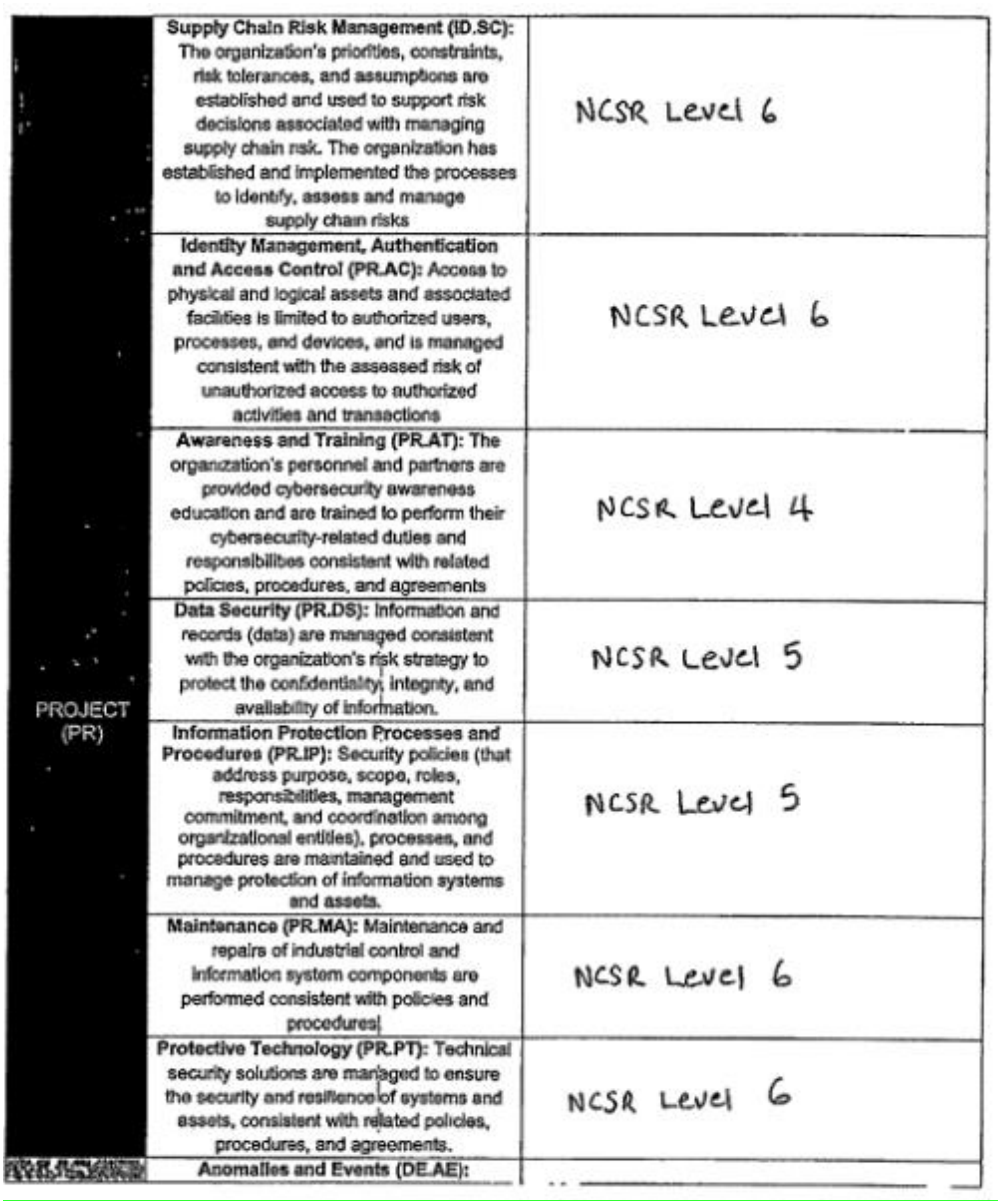
NYC DOE Data Privacy and Security Policies: https://www.schools.nyc.gov/about-us/policies/data-NYC

NYC DOE Parents' Bill of Rights: https://www.schools.nyc.gov/school-life/know-your-rights/parents-bill-of-rights-for-data-privacy-and-security

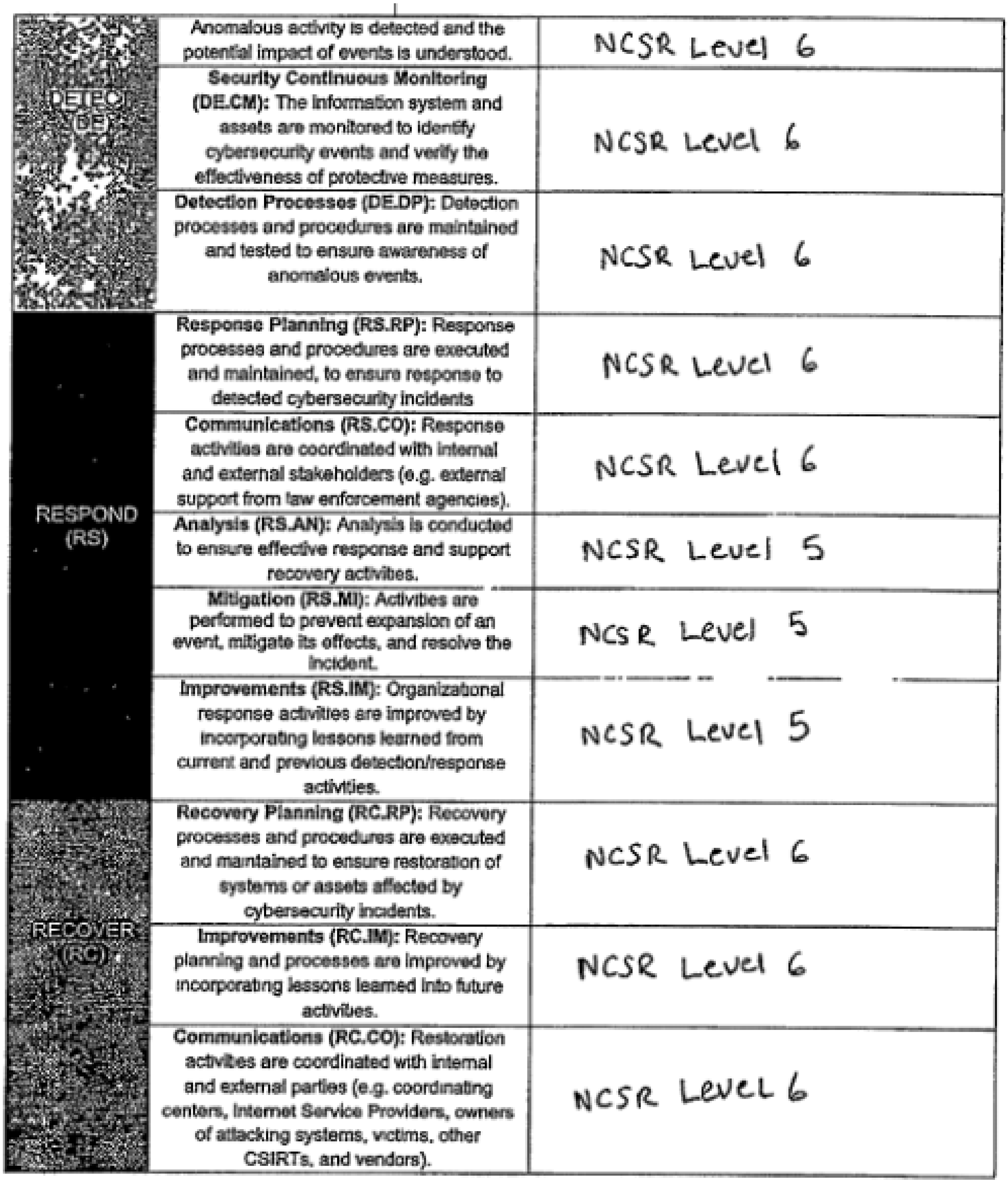
EXHIBIT: NIST CSF TABLE

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 their policies and practices as they align with each category in the Data Privacy and Security Plan template. To complete these sections, a Contractor may: (i) Demonstrate alignment using the National Cybersecurity Review (NCSR) Maturity Scale of 1-7; (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.	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



	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
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	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 activties.	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