BCCS PARENT BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY

DATA PRIVACY AND SECURITY PLAN

Pursuant to Education Law § 2-d and Section 121.6 of the Commissioner's Regulations, Brookville Center for Children's Services (BCCS) is required to have a Data Security and Privacy Plan including alignment with the NIST Cybersecurity Framework, which is the standard for educational agency data privacy and security policies in New York State. Parents (includes legal guardians or persons in parental relationships) and Eligible Students (student 18 years and older) can expect the following.

1	Outline how you will implement applicable data security and privacy contract requirements over the life of the Contract.	Student files are located in a designated file room under lock and key. The files are kept locked at all times and maintained by the Records Management Officer. Each student file contains a folder marked File Access". When a file is taken out, the staff member records the date, file taken out, staff member name, purpose of review, time taken, and time returned. Additionally, any authorized party who obtains access to education records are listed along with the date access was given, and the purpose for which the party is authorized to use these records. Located above the file cabinet is a book called "File Access log". This log contains the same information as the File Access Folder, located in each student's file. While student continues to receive services, all data ls kept in encrypted files at the site. Closed files are maintained in a secure storage facility.
2	Specify the administrative, operational, and technical safeguards and practices that you have in place to protect PII.	BCCS administrative, operational, and technical safeguards include those listed below. Background Check Data Backup Device & Media Controls Disaster Recovery Plan Email Retention Email Usage & Security Emergency Mode Operation Employee ID Badges EPHI Security Incident & Response

		Facility Access Controls Mobile Device Attestation Form Protection from Malicious Software Risk Analysis & Management Security Incident & Reporting Response System Audit Controls Transmission Security Use of Cell Phones & Other Personal Devices User Computer Access Form User Access Management User Authentication & Password Management Work from Home Workplace Security Workstation Security
3	Specify how your officers, employees and subcontractors who have access to PII pursuant to the Service Agreement will receive training on the federal and state laws that govern the confidentiality of PII.	All BCCS employees are trained on federal and state laws regarding confidentiality of PII at the beginning of each school year during orientation. Subcontractors are trained regarding confidentially of student records by their oversight agencies and are beholden to the same standards regarding confidentiality as employees of BCCS.
4	Outline the processes that ensure that your officers, employees, and subcontractors are bound by written agreement to the requirements of the Service Agreement at a minimum.	BCCS' Standards of Conduct for and any subcontractors are bound by written agreement to the confidential information. BCCS has developed policies and procedures in accordance with state and federal rules, including HIPAA & FERPA to assure that the confidentiality of Agency information and information about the people we support is protected and released only with the appropriate authorization or for lawful reasons, in addition to purposes of treatment, payment and operations. All independent contractors should comply with BCCS's privacy policy. All Agency records and information is to be treated as confidential. Confidential information should not be released without the proper authorization. Confidential information includes not only information about the people we support and their families, but also non-public information about the Agency. Contractors are responsible for properly using information stored and produced by all of the Agency's computer systems to the extent they are granted access. Agency information should not be removed from Agency property without permission

		from Department Head or another administrator without proper authority over the information
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.	➢ Policy: Brookville Center for Children's Services shall identify, document, and respond to unauthorized use of the systems that contain electronic protected health information (EPHI). ➢ Procedure: All security incidents, threats to, or violations of, the confidentiality, integrity, or availability of electronic protected health information (EPHI) shall be reported and responded to promptly. **Person(s) Responsibility** All Computer Users 1. Workforce members are responsible to promptly report any potential security related incident to their manager, supervisor, or the HIPAA Security Officer. 2. Incidents that shall be reported include, but are not limited to: 3. EPHI data loss due to disaster, failure, error or theft; 4. Loss of any electronic media that contains EPHI; 5. Loss of the integrity of EPHI; 6. Virus, worm, or other malicious code attacks; 7. Persistent network or system intrusion attempts from a particular entity; 8. Unauthorized access to EPHI on an EPHI based system or network; and 9. Facility incidents, including but not limited to: a. Unauthorized person found in a facility b. Facility break-in c. Lost or stolen key, badge, or cardkey. HIPAA Security Officer/

		IT Department 1. The HIPAA Security Officer, with the assistance of IT Department, shall evaluate the situation to determine if it is a potential security incident, and initiate the response process as required by the type of incident. 2. The HIPAA Security Officer shall receive and record basic information on the incident and forward the information to the appropriate staff for response to that type of incident, i.e., a computer virus incident to the IT staff that provides anti-virus support. 3. The staff shall perform their assigned responsibilities to respond to and/or mitigate any incident consequences. The staff responsible for determining if a possible EPHI breach has resulted from the incident shall notify the HIPAA Security Officer. 4. The HIPAA Security Officer, Compliance Officer and Regulatory Affairs office shall evaluate the incident to determine if a breach of EPHI occurred. If it is determined that a breach has occurred, the incident shall be reported as set forth in the Breach Notification Policies and Procedures. 5. All HIPAA security related incidents and their outcomes will be logged and documented by Regulatory Affairs staff.
6	Describe how data will be transitioned to the [School District] when no longer needed by you to meet your contractual obligations, if applicable.	[School District] requests for data will be sent in compliance with outlined processes to protect student confidentiality. Student files will be retained six years beyond the student's graduation from high school or six years after age 21, whichever is shorter. When data is no longer needed by the school or [School District], the student data will be shredded.
7	Describe your secure destruction practices and how certification will be provided to the [School District].	BCCS Information Technology Department makes use of services provided by eWorks to shred all data

		storage devices at their Freeport, NY location. Certificates are provided by eWorks to confirm that the devices were processed. https://eworksesi.org/contact.html
8	Outline how your data security and privacy program/practices align with the [School District]'s applicable policies.	BCCS' data security and privacy programs and practices align with the [School District] applicable polices. Administrators at each BCCS program are responsible for ensuring confidentiality of any PII. All staff and subcontractors used by the school will keep confidential and make PII maintained at all locations available only for authorized personnel and parents or legal guardians by request. In addition, any digital form of PII will be protected through encryption and the digital security procedures outlined above. When PII is no longer needed, BCCS will dispose of it through shredding. All of these practices ensure compliance with the [School District] applicable policies outlined in this document.
9	Outline how your data security and privacy program/practices materially align with the NIST CSF v1.1 using the Framework chart below.	PLEASE USE TEMPLATE BELOW.

EXHIBIT C.1 – 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 1-7 ; (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	**Function Score ID.AM through ID.SC 5.65** ID.AM-1 7.00 ID.AM-2 7.00 ID.AM-3 6.00

Function	Category	Contractor Response
	importance to organizational objectives and the organization's risk strategy.	ID.AM-4 7.00 ID.AM-5 6.00 ID.AM-6 6.00 **ID.AM Category Score 6.50**
	Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	ID.BE-1 5.00 ID.BE-2 5.00 ID.BE-3 6.00 ID.BE-4 5.00 ID.BE-5 5.00 **ID.BE Category Score 5.20**
	Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	ID.GV-1 6.00 ID.GV-2 6.00 ID.GV-3 6.00 ID.GV-4 6.00 **ID.GV Category Score 6.0**
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	ID.RA-1 6.00 ID.RA-2 6.00 ID.RA-3 6.00 ID.RA-4 6.00 ID.RA-5 5.00 ID.RA-6 5.00 **ID.RA Category Score 5.67**
	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	ID.RM-1 6.00 ID.RM-2 5.00 ID.RM-3 5.00 **ID.RM Category Score 5.33**
	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.	ID.SC-1 5.00 ID.SC-2 5.00 ID.SC-3 5.00 ID.SC-4 6.00 ID.SC-5 5.00 **ID.SC Category Score 5.20**
PROTECT (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.	**Function Score PR.AC through PR.PT 6.18** PR.AC-1 7.00 PR.AC-2 7.00 PR.AC-3 7.00 PR.AC-4 6.00

Function	Category	Contractor Response
		PR.AC-5 6.00 PR.AC-6 6.00 PR.AC-7 7.00 **PR.AC Category Score 6.57**
	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.	PR.AT-1 7.00 PR.AT-2 6.00 PR.AT-3 6.00 PR.AT-4 6.00 PR.AT-5 7.00 **PR.AT Category Score 6.40**
	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	PR.DS-1 6.00 PR.DS-2 6.00 PR.DS-3 7.00 PR.DS-4 6.00 PR.DS-5 6.00 PR.DS-6 5.00 PR.DS-7 6.00 PR.DS-8 6.00 **PR.DS Category Score 6.0**
	Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	PR.IP-1 6.00 PR.IP-2 5.00 PR.IP-3 6.00 PR.IP-4 7.00 PR.IP-5 6.00 PR.IP-6 6.00 PR.IP-7 6.00 PR.IP-8 6.00 PR.IP-9 6.00 PR.IP-10 6.00 PR.IP-11 6.00 PR.IP-12 5.00 **PR.IP Category Score 5.92**
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	PR.MA-1 6.00 PR.MA-2 6.00 **PR. MA Category Score 6.00**
	Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	PR.PT-1 6.00 PR.PT-2 6.00 PR.PT-3 6.00

Function	Category	Contractor Response
		PR.PT-4 6.00 PR.PT-5 7.00 **PR.PT Category Score 6.20**
DETECT (DE)	**Anomalies and Events (DE.AE):** Anomalous activity is detected and the potential impact of events is understood.	**Function Score DE.AE through DE.DP 5.99** DE.AE-1 6.00 DE.AE-2 6.00 DE.AE-3 6.00 DE.AE-4 6.00 DE.AE-5 6.00 **DE.AE Category Score 6.00**
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	DE.CM-1 6.00 DE.CM-2 7.00 DE.CM-3 6.00 DE.CM-4 7.00 DE.CM-5 6.00 DE.CM-6 6.00 DE.CM-7 6.00 DE.CM-8 7.00 **DE.CM Category Score 6.38**
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	DE.DP-1 6.00 DE.DP-2 5.00 DE.DP-3 5.00 DE.DP-4 6.00 DE.DP-5 6.00 **DE.DP Category Score 5.60**
RESPOND (RS)	**Response Planning (RS.RP):** Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.	**Function Score RS.RP through RS.IM 5.76** RS.RP-1 6.00 **RS.RP Category Score 6.00**
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	RS.CO-1 6.00 RS.CO-2 6.00 RS.CO-3 6.00 RS.CO-4 6.00 RS.CO-5 6.00 **RS.CO Category Score 6.00**
	Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.	RS.AN-1 6.00 RS.AN-2 6.00 RS.AN-3 6.00 RS.AN-4 5.00

Function	Category	Contractor Response
		RS.AN-5 6.00 **RS.AN Category Score 5.80**
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	RS.MI-1 6.00 RS.MI-2 6.00 RS.MI-3 6.00 **RS.MI Category Score 6.00**
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	RS.IM-1 5.00 RS.IM-2 5.00 **RS.IM Category Score 5.00**
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.	**Function Score RC.RP through RC.CO 6.17** RC.RP-1 6.00 **RC.RP Category Score 6.00**
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	RC.IM-1 7.00 RC.IM-2 6.00 **RC.IM Category Score 6.50**
	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).	RC.CO-1 6.00 RC.CO-2 6.00 RC.CO-3 6.00 **RC.CO Category Score 6.00**