DATA PRIVACY AND SECURITY PLAN

Provider DATA PRIVACY AND SECURITY PLAN

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

1	Outline how you will implement applicable data security and privacy contract requirements over the life of the Contract.	Provider implements a privacy program aligned with CIS Controls (IG1). We enforce HTTPS encryption, Cloudflare WAF, and automated 3-month data purges. As Cokogames.com is an open-access site requiring no user accounts, data handling is strictly limited to non-PII technical logs and temporary scores
2	Specify the administrative, operational and technical safeguard and practices that you have in place to protect PII.	Although no student PII is collected, we apply CIS-aligned safeguards:Administrative: MFA and restricted access for admins.Operational: Optional Wordwall nicknames are automatically purged within 3 months. No permanent PII databases exist.Technical: TLS/HTTPS, Cloudflare DDoS/WAF protection, and anonymized IP analytics.
3	Address the training received by your employees and any subcontractors engaged in the provision of services under the Contract on the federal and state laws that govern the confidentiality of PII.	All personnel receive annual training on K-12 privacy laws (COPPA, FERPA, state privacy laws). Training emphasizes non-collection practices, secure administration, and confidential handling of server logs.
4	Outline contracting processes that ensure that your employees and any subcontractors are bound by written agreement to the requirements of the Contract, at a minimum.	All employees and subcontractors must sign written agreements requiring strict compliance with state/federal student privacy laws, CIS security standards, and the terms of this Contract prior to system access.
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.	Aligned with CIS Control 17, systems are monitored via Cloudflare WAF and server logs. If a security incident occurs, Provider will contain the threat, notify the EA without unreasonable delay, and supply a complete written incident report.
6	Describe how data will be transitioned to the EA when no longer needed by you to meet your contractual obligations, if applicable.	Not applicable. Provider does not maintain student accounts, profiles, or persistent PII databases. Upon contract end, any remaining session logs are automatically purged during routine maintenance.
7	Describe your secure destruction practices and how certification will be provided to the EA.	Temporary data (Wordwall nicknames, server logs) is securely erased via automated 3-month purge cycles using cryptographic deletion. Provider will issue a formal Certificate of Data Destruction to the EA upon request.
8	Outline how your data security and privacy program/practices align with the EA's applicable policies.	Built on CIS Controls (v8 IG1), Provider's privacy-by-design model (no student accounts, non-personalized ads, Cloudflare WAF protection) fully aligns with EA cybersecurity and student privacy policies.
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 Provider's Data Privacy and Security Plan. Provider should complete the Provider 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 importance to organizational objectives and the organization's risk strategy.	All core assets—including domains, web hosting infrastructure, Cloudflare edge services, and Google Analytics integration—are fully inventoried and managed based on critical availability. No student databases, local physical servers, or student device stores exist within the operational scope.
	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.	Cokogames' mission is to provide free, open-access educational games for K-12 classrooms. Cybersecurity roles and risk management prioritize non-collection of PII, compliance with K-12 privacy laws (COPPA/FERPA/NDPA), and maintaining high platform uptime for schools.
	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.	Formal cybersecurity and data privacy policies govern all platform operations. Compliance with federal/state student privacy mandates, accessibility laws (ADA/WCAG 2.1 AA), and CIS Controls (v8 IG1) is reviewed regularly to manage legal, operational, and regulatory risks.
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	Periodic risk assessments evaluate potential threats to web availability, server configuration, and third-party embeds. Because Cokogames collects no student PII and uses 3-month automated purges for temporary game nicknames, privacy risk to individuals is virtually eliminated.
	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	Risk tolerance is established around strict privacy-by-design principles: zero student accounts, non-personalized classroom advertising, and Cloudflare WAF protection. Operational risk decisions prioritize student privacy and service reliability above all else.
	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	Third-party vendors (Cloudflare, hosting providers, Google Analytics, Wordwall embeds) are evaluated for security standards, encryption, and student privacy compliance. Written agreements and technical controls ensure all external services align with Provider's risk strategy.

Function	Category	Contractor Response
	processes to identify, assess and manage supply chain risks.	
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.	Logical access to hosting, DNS (Cloudflare), and CMS administrative panels is strictly restricted to authorized administrative personnel. Mandatory Multi-Factor Authentication (MFA), role-based access, and strong password policies are enforced. End-users (students/teachers) require no credentials or accounts to access the platform.
	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.	Administrative personnel and contractors receive mandatory annual cybersecurity and student data privacy training (covering COPPA, FERPA, and state privacy laws). Training focuses on secure administrative practices, credential management, non-collection of PII, and incident reporting procedures.
	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.	All data in transit is protected using enforced TLS/HTTPS encryption with HSTS. No student PII is collected or stored. Temporary, non-PII game session artifacts (e.g., Wordwall nicknames) and server logs are managed under automated 3-month cryptographic purge schedules to ensure confidentiality and integrity.
	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.	Security and privacy policies—including backup management, vulnerability patching, and incident response—are maintained and periodically reviewed. Systems follow a privacy-by-design architecture (no student user profiles, non-personalized ads) to manage operational and regulatory risks effectively.
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	System maintenance, software updates, and security patching for server infrastructure and web components are performed remotely via secure, encrypted channels (SSH with key authentication / HTTPS) in alignment with established CIS maintenance procedures.
	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.	Technical security controls include Cloudflare Web Application Firewall (WAF), DDoS mitigation, automated off-site backups, HTTP security headers (nosniff, SAMEORIGIN, Referrer-Policy), and automated log rotation, ensuring continuous system resilience and availability for schools.
DETECT (DE)	**Anomalies and Events (DE.AE):** Anomalous activity is detected and the potential impact of events is understood.	Anomalous web traffic, unauthorized login attempts, and unusual request patterns are automatically detected via Cloudflare WAF and server security logs. Baseline traffic patterns are monitored to quickly identify and evaluate potential operational impacts or security events.
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	Continuous automated monitoring is maintained across all web infrastructure. Cloudflare provides 24/7 edge monitoring for DDoS attacks, malicious bot traffic, and web threats, while server access and error logs are regularly audited to verify the ongoing effectiveness of security controls.
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	Automated alert mechanisms (including Cloudflare security notifications and uptime monitoring) are configured and periodically tested. Detection processes ensure immediate awareness of system anomalies, enabling rapid response to potential service disruptions or threat events.

Function	Category	Contractor Response
RESPOND (RS)	**Response Planning (RS.RP):** Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.	A documented Incident Response Plan aligned with CIS Control 17 is maintained and executed upon detection of any cybersecurity event. The plan outlines clear operational procedures to contain threats, assess system impact, and restore normal service promptly.
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	Response protocols mandate immediate notification to affected Educational Agencies (EAs) in writing without unreasonable delay upon confirmation of a security incident. Communications include detailed event descriptions, affected data elements (if any), and corrective actions taken.
	Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.	Following an anomaly or incident alert, administrative personnel analyze Cloudflare WAF logs, server traffic, and system metrics to determine the root cause, scope of impact, and affected assets, ensuring an effective and targeted recovery process.
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	Threat mitigation activities—including IP blocking, Cloudflare WAF rule adjustments, server patching, and credential rotation—are executed immediately to halt event expansion, isolate affected components, and fully resolve the incident.
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	Post-incident reviews are conducted after any security event or false-positive alert. Lessons learned are incorporated into operational procedures, server firewall rules, and security policies to continuously strengthen platform resilience.
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.	Disaster recovery procedures are maintained to ensure rapid system restoration following any incident. Automated off-site encrypted backups of web files and configurations are executed regularly, enabling full platform restoration to a clean operational state within minimal recovery time objectives (RTO).
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	Following any system recovery or backup restoration test, recovery processes are thoroughly reviewed. Lessons learned are integrated into disaster recovery plans, backup frequencies, and server configuration scripts to optimize future recovery efficiency and platform resilience.
	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).	Restoration activities and operational status updates are coordinated with hosting providers, CDN services (Cloudflare), and affected Educational Agencies (EAs). Formal written confirmation is provided to EAs once systems are fully restored, verified clean, and returned to secure normal operations.