NYSSMA®
A State Unit of NAfME, National Association *for* Music Education

DATA PRIVACY AND CYBERSECURITY FRAMEWORK POLICY

April, 2021

New York State School Music Association (NYSSMA) has chosen to adopt the National Institute of Standards and Technology (NIST) Cybersecurity Framework. This risk-based approach allows NYSSMA to proactively address and better manage cybersecurity risks to its business while the organization continuously evaluates the constantly changing landscape of cyber threats.

The NIST Cybersecurity Framework uses five core functions as the tenants of its framework – Identify, Protect, Detect, Respond and Recover - and NYSSMA has included some of its internal processes in this summary, listed below.

Identify: NYSSMA seeks to continuously evaluate which systems, assets, data and capabilities need to be protected. This evaluation process is owned by the Executive Director.

Protect: NYSSMA takes a layered approach to security and does not believe that any single service, device or software is capable of complete protection. Individual protections include, but are not limited to:

- NYSSMA employees are trained in basic security principles and to recognize social engineering techniques
- All NYSSMA servers, computers and laptops have antivirus software and managed detection and response software installed to continuously monitor for malicious behavior and activity
- All NYSSMA servers, computers and laptops are kept up to date with the latest security and critical patches, applied on a rolling basis
- NYSSMA uses hardware firewall appliances at its network gateway as well as a dedicated VPN appliance to provide secure remote access that is encrypted
- All NYSSMA servers and critical business data are backed up on a rolling basis throughout each day with encrypted copies stored offsite in redundant data centers
- NYSSMA has a secure password and authentication policy in place, including for its wireless networks
- NYSSMA employs the use of multifactor authentication in front of all sources of data, including email access and its internal network resources
- NYSSMA limits employee access to specific data required for specific functions
- NYSSMA controls physical access to its computers and network infrastructure

Dr. David A. Gaines, Executive Director, 718 The Plain Road, Westbury, NY 11590-5956
Phone: 516-997-7200 ext. 10 • Fax: 516-997-1700 • Email: executive@nyssma.org • Website: www.nyssma.org

Detect: NYSSMA continuously monitors its security services and physical network, looking for anomalies and other events that may present potential security issues. Any detected events are analyzed and processes are continually improved based on new information gathered.

Respond: It is the policy of NYSSMA to respond to each cybersecurity event on a case-by-case basis, taking into consideration the specific circumstances and extent to which the event occurred. In order to best protect NYSSMA and its clients, all qualifying events are to be reported to the Executive Director to ensure that a response plan is initiated, should it be deemed necessary. A response plan includes, but is not limited to:

- Communication with relevant stakeholders or other key personnel, including status updates as needed

- Taking steps to immediately quarantine any breach or incident to mitigate impact

- Studying each incident to incorporate lessons learned, updating strategies accordingly

Recover: NYSSMA plans to recover from a cybersecurity event either during or after an incident. Aside from addressing and mitigating the specific circumstances of each incident, NYSSMA maintains a Business Continuity and Disaster Recovery plan to address any significant business disruptions that may occur.

8 NYCRR Part 121	
121.2 Each educational agency shall ensure that it has provisions in its contracts with third party contractors or in separate data sharing and confidentiality agreements that require the confidentiality of shared student data or teacher or principal data be maintained in accordance with Federal and State law and the educational agency's data security and privacy policy.	
121.3(b) The bill of rights shall also be included with every contract an educational agency enters with a third-party contractor that receives personally identifiable information. The supplemental information must be developed by the educational agency and include the following Information:	
121.3(b)(1) What is the exclusive purposes for which the student data or teacher or principal data will be used, as defined in the contract?	NYSSMA uses student data for selection of students in honor ensembles and student evaluations.
121.3(b)(2)Will the organization use subcontractors? If so, how will the organization ensure that the subcontractors, or other authorized persons or entities to whom the third-party contractor will disclose the student data or teacher or principal data, if any, will abide by all applicable data protection and security requirements, including but not limited to those outlined in applicable State and Federal laws and regulations (e.g., FERPA; *Education Law section 2-d*)?	Yes – NYSSMA will use subcontractors. NYSSMA will obtain contracts with it's subcontractors including data confidentiality requirements as well as compliance with Ed Law 2-d, 8 NYCRR Part 121 and the NIST CSF.
121.3(b)(3) **What is the** duration of the contract including the contract's expected commencement and expiration date? Describe what will happen to the student data or teacher or principal data upon expiration of the contract or other written agreement (e.g., whether, when and in what format it will be returned to the educational agency, and/or whether, when and how the data will be destroyed).	NYSSMA does contract directly with school districts through it's student registration process. The duration of the contract is year to year and commences as districts participate and terminate when the event is over. The duration of the contract is determined on an event by event basis. The contract commences on July 1, and terminates on June 30th of each year. When the engagement with the district terminates, NYSSMA will return or destroy the data at the direction of the school district.

121.3(b)(4) how can a parent, student, eligible student, teacher or principal challenge the accuracy of the student data or teacher or principal data that is collected;?	Parents or eligible students can challenge the accuracy of any Protected Data provided by a Participating Educational Agency to NYSSMA, by contacting the student's district of residence regarding procedures for requesting amendment of education records under the Family Educational Rights and Privacy Act (FERPA).
121.3(b)(5) Describe where the student data or teacher or principal data will be stored, described in such a manner as to protect data security, and the security protections taken to ensure such data will be protected and data security and privacy risks mitigated.	The data is stored locally on servers and on two offsite data centers, one in Pennsylvania and the other in Utah. The data is encrypted at rest and in-transit, remote access to the data is secured by multi-factor identification, the least privileged access policy is in place. There is a secure password policy and password rotation policy in place.
(6)address how the data will be protected using encryption while in motion and at rest.	The server itself the data volume is encrypted on the physical server and the back up technology is also encrypted. It is encrypted in transit back to those data centers. Staff laptops are encrypted.
121.6(a)Please submit the organization's data security and privacy plan that is accepted by the educational agency.	See attached.
121.6(a)(1) **Describe how the organization** will implement all State, Federal, and local data security and privacy contract requirements over the life of the contract, consistent with the educational agency's data security and privacy policy;	NYSSMA affirmatively states that it will maintain compliance with all State and Federal and local data security and privacy contract requirements consistent with the educational agency's data security and privacy policy.
121.6(a)(2)specify the administrative, operational and technical safeguards and practices it has in place to protect personally identifiable information that it will receive under the contract;	The data is encrypted at rest and in-transit, remote access to the data is secured by multi-factor identification, the least privileged access policy is in place. There is a secure password policy and password rotation policy in place. Please refer to the "Protect" section of the NYSSMA data privacy policy.
121.6(a)(3)demonstrate that the organization complies with the requirements of section 121.3(c) of this Part	NYSSMA will sign the education agency's Parent Bill of Rights.
121.6(a)(4)specify how officers or employees of the organization and its assignees who have	Refer to privacy policy. NYSSMA uses the "KnowBe4" training platform.

Dr. David A. Gaines, Executive Director, 718 The Plain Road, Westbury, NY 11590-5956
Phone: 516-997-7200 ext. 10 • Fax: 516-997-1700 • Email: executive@nyssma.org • Website: www.nyssma.org

access to student data, or teacher or principal data receive or will receive training of the Federal and State laws governing confidentiality of such data prior to receiving access;	
121.6(a)(5)specify if the organization will utilize sub-contractors and how it will manage those relationships and contracts to ensure personally identifiable information is protected;	Sub-contractors are used to process student data for the purposes of evaluation and honors ensemble participation. Sub-contractor management is defined in the privacy policy.
121.6(a)(6)specify how the organization will manage data security and privacy incidents that implicate personally identifiable information including specifying any plans to identify breaches and unauthorized disclosures, and to promptly notify the educational agency;	The educational agency will be promptly notified of a breaches and unauthorized disclosure by the NYSSMA Executive Director. Breach management is defined in the privacy policy.
121.6(a)(7)describe whether, how and when data will be returned to the educational agency, transitioned to a successor contractor, at the educational agency's option and direction, deleted or destroyed by the third-party contractor when the contract is terminated or expires.	The school district will be notified of any transition to a successor contractor and data will be deleted or returned to the educational agency at the request of the school district.
121.9(a) In addition to all other requirements for third-party contractors set forth in this Part, each third-party contractor that will receive student data or teacher or principal data shall:	
121.9(a)(1) describe the organization's adopted technologies, safeguards and practices that align with the NIST Cybersecurity Framework;	NYSSMA aligns with the NIST CSF. Refer to the privacy policy.
121.9(a)(2)Describe how the organization will comply with the data security and privacy policy of the educational agency with whom it contracts; *Education Law section 2-d*; and this Part;	Refer to the privacy policy.
121.9(a)(3) Describe how the organization will limit internal access to personally identifiable information to only those employees or sub-contractors that need access to provide the contracted services;	Refer to privacy policy.
121.9(a)(4)Describe how the organization will control access to the protected data and not use the personally identifiable information for any purpose not explicitly authorized in its contract;	Refer to the privacy policy. NYSSMA will only use student data for evaluations and honors ensembles.
121.9(a)(5)Describe how the organization will not disclose any personally identifiable information to any other party without the prior written consent of the parent or eligible student;	NYSSMA will not disclose any personally identifiable information to any other party with out prior written consent, except to the extent

(i)except for authorized representatives of the third-party contractor such as a subcontractor or assignee to the extent they are carrying out the contract and in compliance with State and Federal law, regulations and its contract with the educational agency; or **(ii)**unless required by statute or court order and the third-party contractor provides a notice of disclosure to the department, district board of education, or institution that provided the information no later than the time the information is disclosed, unless providing notice of disclosure is expressly prohibited by the statute or court order.	that it is complying with State or Federal law, or regulation, unless required to do so by statute or court order.
121.9(a)(6)Describe how the organization will maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of personally identifiable information in its custody;	Refer to privacy policy.
121.9(a)(7) Describe how the organization will use encryption to protect personally identifiable information in its custody while in motion or at rest; and	The server itself the data volume is encrypted on the physical server and the back up technology is also encrypted. It is encrypted in transit back to those data centers. Staff laptops are encrypted.
121.9(a)(8)Affirmatively state that the organization shall not sell personally identifiable information nor use or disclose it for any marketing or commercial purpose or permit another party to do so.	NYSSMA will not sell personally identifiable information and will not use or disclose the information for any marketing or commercial purpose or permit another party to do so.
121.9(a)(b) Describe how the organization will supervise its subcontractors to ensure that as subcontractors perform its contractual obligations, the subcontractor will conform with obligations imposed on the third-party contractor by State and Federal law to keep protected data secure.	Refer to privacy policy.
121.10(a) Describe how the organization shall promptly notify each educational agency with which it has a contract of any breach or unauthorized release of personally identifiable information in the most expedient way possible and without unreasonable delay but no more than seven calendar days after the discovery of such breach.	NYSSMA will promptly notify the school district, without unreasonable delay and within seven calendar days after the discovery of the breach in the most expedient manner possible.
121.10(c) Affirmatively state that the organization will cooperate with educational	NYSSMA will cooperate with educational agencies and law enforcement to protect the

agencies and law enforcement to protect the integrity of investigations into the breach or unauthorized release of personally identifiable information.	integrity of investigations into the breach or unauthorized release of personally identifiable information.
121.10(f) Affirmatively state that where a breach or unauthorized release is attributed to the organization, the organization shall pay for or promptly reimburse the educational agency for the full cost of such notification.	NYSSMA will pay for or promptly reimburse the educational agency for the full cost of such notification.