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.