NEW YORK COUNCIL
NAVY LEAGUE *of the* US
Citizens in Support of the Sea Services

Written Information Security Program (WISP)

The objectives of this comprehensive written information security program ("WISP") include defining, documenting and supporting the implementation and maintenance of the administrative, technical and physical safeguards the New York Council Navy League Inc., hereinafter "NYNL", has selected to protect the personal information it collects, creates, uses and maintains. This WISP has been developed in accordance with the requirements of the The Stop Hacks and Improve Electronic Data Security (SHIELD) Act, General Business Law 899-aa.

In the event of a conflict between this WISP and any legal obligation or other NYNL policy or procedure, the provisions of this WISP shall govern, unless the Information Security Coordinator specifically reviews, approves, and documents an exception (see Section 3).

1. Purpose. The purpose of this WISP is to:

(a) Ensure the security, confidentiality, integrity and availability of personal and other sensitive information NYNL collects, creates, uses and maintains.

(b) Protect against any anticipated threats or hazards to the security, confidentiality, integrity or availability of such information.

(c) Protect against unauthorized access to or use of NYNL-maintained personal and other sensitive information that could result in substantial harm or inconvenience to any constituent or employee.

(d) Define an information security program that is appropriate to NYNL's size, scope and business, its available resources, and the amount of personal and other sensitive information that NYNL owns or maintains on behalf of others, while recognizing the need to protect both constituent and employee information.

2. Scope. This WISP applies to all employees, contractors, vendors, volunteers, officers and directors of NYNL. It applies to any records that contain personal or other sensitive information in any format and on any media, whether in electronic or paper form.

(a) For purposes of this WISP, "personal information" means either a US resident's first and last name or first initial and last name in combination with any one or more of the following data elements, or any of the following data elements standing alone or in combination, if such data elements could be used to identify or commit identity theft against the individual:

(i) Social Security number;

(ii) Driver's license number, other government-issued identification number, including passport number, or tribal identification number;

(iii) Account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password that would permit access to the individual's financial account.

(iv) Health information, including information regarding the individual's medical history or mental or physical condition, or medical treatment or diagnosis by a health care professional, created or received by NYNL;

(v) Health insurance identification number, subscriber identification number or other unique identifier used by a health insurer;

(vi) Email address with any required security code, access code or password that would permit access to an individual’s personal, medical, insurance or financial account; or

(vii) Any information permitting the physical or online contacting of a specific individual, to include but not limited to phone number, email, physical address or direct messages on social media platforms.

(b) Personal information does not include lawfully obtained information that is available to the general public, including publicly available information from federal, state or local government records.

(c) For purposes of this WISP, “sensitive information” means data that:

(i) NYNL considers to be highly confidential information; or

(ii) If accessed by or disclosed to unauthorized parties, could cause significant or material harm to NYNL, its constituents or its business partners.

Sensitive information includes, but is not limited to, personal information. If you have questions regarding what is included in sensitive information, you may request a copy of the NYNL Information Security Policy by request from the Information Security Coordinator(s).

3. Information Security Coordinator(s). NYNL has designated a Council Officer to implement, coordinate and maintain this WISP (the “Information Security Coordinator”). The Information Security Coordinator (ISC), in collaboration with NYNL staff shall be responsible for:

(a) Initial implementation of this WISP, including:

(i) Assessing internal and external risks to personal and other sensitive information and maintaining related documentation, including risk assessment reports and remediation plans (see Section 4);

(ii) Coordinating the development, distribution and maintenance of information security policies and procedures (see Section 5), including identifying data stewards who will receive initial requests to sensitive information that is stored, created or maintained by the NYNL;

(iii) Coordinating the design of reasonable and appropriate administrative, technical and physical safeguards to protect personal and other sensitive information (see Section 6);

(iv) Ensuring that the safeguards are implemented and maintained to protect personal and other sensitive information throughout NYNL, where applicable (see Section 6);

(v) Collaborating with staff to manage service providers that access or maintain personal and other sensitive information on behalf of NYNL (see Section 7);

(vi) Monitoring and testing the information security program's implementation and effectiveness on an annual basis (see Section 8);

(vii) Defining and managing incident response procedures (see Section 9) and;

(viii) Establishing and managing enforcement policies and procedures for this WISP, in collaboration with NYNL staff and Directors (see Section 10)

(b) Employee, contract employee and (as applicable) stakeholder training, including:

(i) Providing annual training regarding this WISP, NYNL's safeguards, and relevant information security policies and procedures for all employees, contract employee, vendor and (as applicable) stakeholders who have or may have access to personal or other sensitive information;

(ii) Ensuring that training attendees formally acknowledge their receipt and understanding of the training and related documentation, through written acknowledgement forms; and

(iii) Retaining training and acknowledgment records.

(c) Reviewing this WISP and the security measures defined here at least annually, or whenever there is a material change in NYNL's business practices that may reasonably implicate the security, confidentiality, integrity or availability of records containing personal or other sensitive information (see Section 11).

(d) Defining and managing an exceptions process to review, approve or deny, document, monitor and periodically reassess any necessary and appropriate business-driven requests for deviations from this WISP or NYNL's information security policies and procedures.

(e) Annually reporting to NYNL Directors regarding the status of the information security program and NYNL's safeguards to protect personal and other sensitive information.

4. Risk Assessment. As a part of developing and implementing this WISP, NYNL will conduct a periodic documented risk assessment, at least annually, or whenever there is a material change in NYNL's business practices that may implicate the security, confidentiality, integrity or availability of records containing personal or other sensitive information.

(a) The risk assessment shall:

(i) Identify reasonably foreseeable internal and external risks to the security, confidentiality, integrity or availability of any electronic, paper or other records containing personal or other sensitive information;

(ii) Assess the likelihood and potential damage that could result from such risks, taking into consideration the sensitivity of the personal and other sensitive information; and

(iii) Evaluate the sufficiency of relevant policies, procedures, systems and safeguards in place to control such risks, in areas that include, but may not be limited to:

(A) Employee, contractor, vendor and (as applicable) stakeholder training and management;

(B) Employee, contractor, vendor and (as applicable) stakeholder compliance with this WISP and related policies and procedures;

(C) Information systems, including network, computer and software acquisition, design, implementation, operations and maintenance, as well as data processing, storage, transmission, retention and disposal; and

(D) NYNL's ability to prevent, detect and respond to attacks, intrusions and other security incidents or system failures.

(b) Following each risk assessment, NYNL will:

(i) Design, implement and maintain reasonable and appropriate safeguards to minimize identified risks;

(ii) Reasonably and appropriately address any identified gaps; and

(iii) Periodically monitor the effectiveness of NYNL's safeguards, as specified in this WISP (see Section 8).

5. Information Security Policies and Procedures. As part of this WISP, NYNL will develop, maintain and distribute information security policies and procedures in accordance with applicable laws and standards to relevant employees, contract employee and (as applicable) other stakeholders to:

(a) Establish policies regarding:

(i) Information classification;

(ii) Information handling practices for personal and other sensitive information, including the storage, access, disposal and external transfer or transportation of personal and other sensitive information;

(iii) User access management, including identification and authentication (using passwords or other appropriate means);

(iv) Encryption;

(v) Computer and network security;

(vi) Physical security;

(vii) Incident reporting and response;

(viii) Employee, contract employee and volunteer use of technology, including acceptable use; and

(ix) Information systems acquisition, development, operations and maintenance.

(b) Detail the implementation and maintenance of NYNL's administrative, technical and physical safeguards (see Section 6).

6. Safeguards. NYNL will develop, implement and maintain reasonable administrative, technical and physical safeguards in accordance with applicable laws and standards to protect the security, confidentiality, integrity and availability of personal or other sensitive information that NYNL owns or maintains on behalf of others.

(a) Safeguards shall be appropriate to NYNL's size, scope and business, its available resources and the amount of personal and other sensitive information that NYNL owns or maintains on behalf of others, while recognizing the need to protect both constituent and employee information.

(b) NYNL shall document its administrative, technical and physical safeguards in NYNL's information security policies and procedures (see Section 5).

(c) NYNL's administrative safeguards shall include, at a minimum:

(i) Designating an ISC to coordinate the information security program (see Section 3);

(ii) Identifying reasonably foreseeable internal and external risks, and assessing whether existing safeguards adequately control the identified risks (see Section 4);

(iii) Training employees in security program practices and procedures, with ISC oversight (see Section 3);

(iv) Selecting service providers that are capable of maintaining appropriate safeguards, and requiring service providers to maintain safeguards by contract (see Section 7); and

(v) Adjusting the information security program in light of business changes or new circumstances (see Section 11).

(d) NYNL's technical safeguards shall include maintenance of a security system covering its network (including wireless capabilities) and computers that, at a minimum, and to the extent technically feasible, supports:

(i) Secure user authentication protocols, including:

(A) Controlling user identification and authentication with a reasonably secure method of assigning and selecting passwords (ensuring that passwords are kept in a location or format that does not compromise security);

(B) Restricting access to active users and active user accounts only and preventing terminated employees, contract employee or volunteers from accessing systems or records; and

(C) Blocking a particular user identifier's access after multiple unsuccessful attempts to gain access or placing limitations on access for the particular system.

(ii) Secure access control measures, including:

(A) Restricting access to records and files containing personal or other sensitive information to those with a need to know to perform their duties; and

(B) Assigning to each individual with computer or network access unique identifiers and passwords (or other authentication means, but not vendor-supplied default passwords) that are reasonably designed to maintain security.

(iii) Encryption or password protection of financially sensitive information traveling wirelessly or across public networks;

(iv) Encryption or password protection of all personal or other sensitive information stored on laptops or other devices, and to the extent technically feasible, personal or other sensitive information stored on any other device or media (data-at-rest);

(v) Reasonable system monitoring for preventing, detecting and responding to unauthorized use of or access to personal or other sensitive information or other attacks or system failures;

(vi) Reasonably current firewall protection and software patches for systems that contain (or may provide access to systems that contain) personal or other sensitive information; and

(vii) Reasonably current system security software (or a version that can still be supported with reasonably current patches and malicious software ("malware") definitions) that (1) includes malware protection with reasonably current patches and malware definitions, and (2) is configured to receive updates on a regular basis.

(e) NYNL's physical safeguards shall, at a minimum, provide for:

(i) Defining and implementing reasonable physical security measures to protect areas where personal or other sensitive information may be accessed, including reasonably restricting physical access and storing records containing personal or other sensitive information in locked facilities, areas, or containers;

(ii) Preventing, detecting, and responding to intrusions or unauthorized access to personal or other sensitive information, including during or after data collection, transportation or disposal; and

(iii) Secure disposal or destruction of personal or other sensitive information, whether in paper or electronic form, when it is no longer to be retained in accordance with applicable laws or accepted standards.

7. Service Provider Oversight. NYNL will oversee each of its service providers that may have access to or otherwise create, collect, use or maintain personal or other sensitive information on its behalf by:

(a) Evaluating the service provider's ability to implement and maintain appropriate security measures, consistent with this WISP and all applicable laws and NYNL's obligations.

(b) Requiring the service provider by contract to implement and maintain reasonable security measures, consistent with this WISP and all applicable laws and NYNL's obligations.

(c) Monitoring and auditing the service provider's performance to verify compliance with this WISP and all applicable laws and NYNL's obligations.

8. Monitoring. NYNL will annually test and monitor the implementation and verify effectiveness of its information security program to ensure that it is operating in a manner reasonably calculated to prevent unauthorized access to or use of personal or other sensitive information. NYNL shall reasonably and appropriately address any identified gaps.

9. Incident Response. NYNL will establish and maintain policies and procedures regarding information security incident response (see Section 5). Such procedures shall include:

(a) Documenting the response to any security incident or event that involves a breach of security.

(b) Performing a post-incident review of events and actions taken.

(c) Reasonably and appropriately addressing any identified gaps.

10. Enforcement. Violations of this WISP may result in disciplinary actions by the Executive Committee.

11. Program Review. NYNL will review this WISP and the security measures defined herein at least annually, or whenever there is a material change in NYNL's business practices that may reasonably implicate the security, confidentiality, integrity or availability of records containing personal or other sensitive information.

(a) NYNL shall retain documentation regarding any such program review, including any identified gaps and action plans.

Effective Date. This WISP is effective as of September 17, 2020.

Revision History: Original publication August 10, 2020.

ACKNOWLEGMENT FORM FOLLOWS

APPENDIX

WRITTEN INFORMATION SECURITY PROGRAM (WISP) ACKNOWLEGMENT FORM

ACKNOWLEDGMENT OF RECEIPT AND REVIEW

I acknowledge that I received and read a copy of NYNL's Written Information Security Program (WISP), dated September 17, 2020 and understand that it is my responsibility to be familiar with and abide by its terms. I understand that the information contained therein is intended to help NYNL's stakeholders work together effectively to manage information security risks as part of their assigned position responsibilities. The WISP is not promissory and does not set terms or conditions of employment nor does it create an employee contract.

____

Signature

____

Printed Name

____

Date