JEFFERSON • LEWIS • HAMILTON • HERKIMER • ONEIDA

BOARD OF COOPERATIVE EDUCATIONAL SERVICES

Contract Addendum

Protection of Student, Teacher, and Principal Data

1. Applicability of this Addendum

The Jefferson, Lewis, Hamilton, Herkimer, Oneida BOCES ("BOCES"), an educational agency, and National Restaurant Association Solutions, LLC ("Vendor") are parties to a purchase order dated [DATE] ("the underlying contract") governing the terms under which BOCES accesses, and Vendor provides, online instructional courses and exams for food safety industry-based certifications, purchased per student. ("Product"). BOCES' use of the Product results in Vendor receiving student, teacher, or principal personally identifiable information as defined in federal and state statute, including New York Education Law Section 2-d and this Addendum. The terms of this Addendum shall amend and modify the underlying contract and shall have precedence over terms set forth in the underlying contract and any online Terms of Use or Service published by Vendor.

2. Definitions

2.1. "Assignee" and "Subcontractor" shall each mean any person or entity that receives, stores, or processes "Protected Information" covered by this Contract from Vendor for the purpose of enabling or assisting Vendor to deliver the product or services covered by this Contract.

2.2. "This Contract" means the underlying contract as modified by this Addendum.

2.3. "Protected Information", as applied to student data, means "personally identifiable information" as defined in 34 CFR Section 99.3 implementing the Family Educational Rights and Privacy Act (FERPA) where that information is received by Vendor from BOCES or is created by the Vendor's product or service in the course of being used by BOCES. "Protected Information", as applied to Teacher or Principal Data means personally identifiable information from the records of an educational agency relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of Education Law §§3012-c and 3012-d.

2.4. "Breach" means the unauthorized acquisition, access, use, or disclosure of student data and/or teacher or principal data by or to a person not authorized to acquire, access, use, or receive the student data and/or teacher or principal data.

3. Vendor Status

Vendor acknowledges that for purposes of New York State Education Law Section 2-d it is a third- party contractor, and that for purposes of any Protected Information that constitutes education records under the Family Educational Rights and Privacy Act (FERPA) in performing its services under this Contract, it is a school official with a legitimate educational interest in the educational records.

4. Confidentiality of Protected Information

Vendor agrees that the confidentiality of Protected Information that it receives, processes, or stores will be handled in accordance with all state and federal laws that protect the confidentiality of Protected Information, and in accordance with the BOCES Policies on Data Security and Privacy and the Parent's Bill of Rights for Data Privacy and Security, copies of which are Attachment B to this Addendum; provided, however, that Vendor may disclose certain Protected Information in accordance with Attachment D to this Addendum.

5. Vendor Employee Training

Vendor agrees that any of its officers or employees, and any officers or employees of any Assignee of Vendor, who have access to Protected Information will receive training on the federal and state law governing confidentiality of such information prior to receiving access to that information.

6. No Use of Protected Information for Commercial or Marketing Purposes

Vendor warrants that Protected Information received by Vendor from BOCES or by any Assignee of Vendor, shall not be sold or used for any commercial or marketing purposes; shall not be used by Vendor or its Assignees for purposes of receiving remuneration, directly or indirectly; shall not be used by Vendor or its Assignees for advertising purposes; shall not be used by Vendor or its Assignees to develop or improve a product or service; and shall not be used by Vendor or its Assignees to market products or services to students.

7. Ownership and Location of Protected Information

7.1. Ownership of all Protected Information that is disclosed to or held by Vendor shall remain with BOCES. Vendor shall acquire no ownership interest in education records or Protected Information.

7.2. As permitted under applicable law, BOCES shall have access to the BOCES' Protected Information at all times through the term of this Contract. As permitted under applicable law, BOCES shall have the right to import or export Protected Information in piecemeal or in its entirety at their discretion, without interference from Vendor.

7.3. Other than as required by Vendor as part of its of standard security policies, Vendor is prohibited from data mining, cross tabulating, and monitoring data usage and access by BOCES or its authorized users, or performing any other data analytics other than those required to provide the Product to BOCES. Vendor is allowed to perform industry standard back-ups of Protected Information. Documentation of back-up must be provided to BOCES upon reasonable request.

7.4. All Protected Information shall remain in the continental United States (CONUS) or Canada. Any Protected Information stored, or acted upon, must be located solely in data centers in CONUS or Canada. Services which directly or indirectly access Protected Information may only be performed from locations within CONUS or Canada.

8. Purpose for Sharing Protected Information

The exclusive purpose for which Vendor is being provided access to Protected Information is to provide the product or services that are the subject of this Contract to BOCES.

9. Downstream Protections

Vendor agrees that, in the event that Vendor subcontracts with or otherwise engages another entity in order to fulfill its obligations under this Contract, including the purchase, lease, or sharing of server space owned by another entity, that entity shall be deemed to be an “Assignee” of Vendor for purposes of Education Law Section 2-d, and Vendor will only share Protected Information with such entities if those entities are contractually bound to observe all applicable New York State and federal laws.

10. Protected Information and Contract Termination

10.1. The expiration date of this Contract is defined by the underlying contract.

10.2. Upon expiration of this Contract without a successor agreement in place, Vendor shall assist BOCES in exporting all Protected Information previously received from, or then owned by, BOCES.

10.3. Vendor shall thereafter securely delete and overwrite any and all Protected Information remaining in the possession of Vendor or its assignees or subcontractors (including all hard copies, archived copies, electronic versions or electronic imaging of hard copies of shared data) as well as any and all Protected Information maintained on behalf of Vendor in secure data center facilities.

10.4. Vendor shall ensure that no copy, summary or extract of the Protected Information or any related work papers are retained on any storage medium whatsoever by Vendor, its subcontractors or assignees, or the aforementioned secure data center facilities.

10.5. To the extent that Vendor and/or its subcontractors or assignees may continue to be in possession of any de-identified data (data that has had all direct and indirect identifiers removed) derived from Protected Information, they agree not to attempt to re-identify de-identified data and not to transfer de-identified data to any party.

10.6. Upon reasonable request, Vendor and/or its subcontractors or assignees will provide a certification to BOCES from an appropriate officer that the requirements of this paragraph have been satisfied in full.

10.7. Notwithstanding anything to the contrary contained herein, Vendor may retain Protected Information to the extent reasonably necessary to comply with applicable laws and regulations or guidelines provided by an accreditation body (including but not limited to the American National Standards Institute).

11. Data Subject Request to Amend Protected Information

11.1. In the event that a parent, student, or eligible student wishes to challenge the accuracy of Protected Information that qualifies as student data for purposes of Education Law Section 2-d, that challenge shall be processed through the procedures provided by the BOCES for amendment of education records under the Family Educational Rights and Privacy Act (FERPA).

11.2. Vendor will reasonably cooperate with BOCES in retrieving and revising Protected Information, but shall not be responsible for responding directly to the data subject.

12. Vendor Data Security and Privacy Plan

12.1. Vendor agrees that for the life of this Contract the Vendor will maintain the administrative, technical, and physical safeguards described in the Data Security and Privacy Plan set forth in Attachment C to this Contract and made a part of this Contract.

12.2. Vendor warrants that the conditions, measures, and practices described in the Vendor's Data Security and Privacy Plan:

a. align with the NIST Cybersecurity Framework 1.0;

b. equal industry best practices including, but not necessarily limited to, disk encryption, file encryption, firewalls, and password protection;

c. outline how the Vendor will implement all state, federal, and local data security and privacy contract requirements over the life of the contract, consistent with the BOCES data security and privacy policy (Attachment B);

d. specify the administrative, operational and technical safeguards and practices it has in place to protect Protected Information that it will receive under this Contract;

e. demonstrate that it complies with the requirements of Section 121.3(c) of Strengthening Data Privacy and Security in NY State Educational Agencies to Protect Personally Identifiable Information;

f. specify how officers or employees of the Vendor and its assignees who have access to Protected Information receive or will receive training on the federal and state laws governing confidentiality of such data prior to receiving access;

g. specify if the Vendor will utilize sub-contractors and how it will manage those relationships and contracts to ensure Protected Information is protected;

h. specify how the Vendor will manage data security and privacy incidents that implicate Protected Information including specifying any plans to identify breaches and unauthorized disclosures, and to promptly notify BOCES; and

i. describe whether, how and when data will be returned to BOCES, transitioned to a successor contractor, at BOCES' option and direction, deleted or destroyed by the Vendor when the contract is terminated or expires.

13. Additional Vendor Responsibilities

Vendor acknowledges that under Education Law Section 2-d and related regulations it has the following obligations with respect to any Protected Information, and any failure to fulfill one of these statutory obligations may subject the vendor to a monetary civil penalty and shall be a breach of this Contract:

13.1. Vendor shall limit internal access to Protected Information to those individuals and Assignees or subcontractors that need access to provide the contracted services;

13.2. Vendor will not use Protected Information for any purpose other than those explicitly authorized in this Contract, including Attachment D to this Addendum;

13.3. Vendor will not disclose any Protected Information to any party who is not an authorized representative of the Vendor using the information to carry out Vendor's obligations under this Contract or to the BOCES unless (1) Vendor has the prior written consent of the parent or eligible student to disclose the information to that party, or (ii) the disclosure is required by statute or court order, and notice of the disclosure is provided to BOCES no less than three (3) business day prior to disclosure, unless such notice is expressly prohibited by the statute or court order;

13.4. Vendor will maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of Protected Information in its custody;

13.5. Vendor will use encryption technology to protect data while in motion or in its custody from unauthorized disclosure using a technology or methodology specified by the secretary of the U S. Department of HHS in guidance issued under P.L. 111-5, Section 13402(H)(2);

13.6. Vendor will notify the BOCES of any breach of security resulting in an unauthorized release of student data by the Vendor or its Assignees in violation of state or federal law, or of contractual obligations relating to data privacy and security in the most reasonably expedient way possible and without unreasonable delay but no more than seven calendar days after the discovery of the breach; and

13.7. To the extent required by law, where a breach or unauthorized disclosure of Protected Information is attributed to the Vendor, the Vendor shall pay for or promptly reimburse BOCES for the full cost incurred by BOCES to send notifications required by Education Law Section 2-d.

13.8. BOCES acknowledges and agrees to the terms of Attachment D to this Addendum.

Dated: June 20, 2024

Michele A. Carpenter

For the Jefferson-Lewis BOCES

Alsha Gulden 06/17/2024

For the Vendor

BOARD OF COOPERATIVE EDUCATIONAL SERVICES

Attachment A - Supplemental Information about this Contract

CONTRACTOR	National Restaurant Association Solutions, LLC
PRODUCT	
PURPOSE DETAILS	The exclusive purpose for which Vendor is being provided access to Protected Information is to provide the product or services that are the subject of this Contract to BOCES. The product or services are used to provide culinary arts instruction.
SUBCONTRACTOR DETAILS	Vendor represents that it will only share Protected Information with subcontractors if those subcontractors are contractually bound to observe the same obligations to maintain the privacy and security of Protected Information as are required under all applicable New York State and federal laws.
DATA DESTRUCTION INFORMATION	The agreement expires [DATE OF EXPIRATION]. Upon expiration of this Contract without a successor agreement in place, Vendor shall assist BOCES in exporting all Protected Information previously received from, or then owned by, BOCES. Vendor shall thereafter securely delete and overwrite any and all Protected Information remaining in the possession of Vendor or its assignees or subcontractors (including all hard copies, archived copies, electronic versions or electronic imaging of hard copies of shared data) as well as any and all Protected Information maintained on behalf of Vendor in secure data center facilities. Vendor shall ensure that no copy, summary or extract of the Protected Information or any related work papers are retained on any storage medium whatsoever by Vendor, its subcontractors or assignees, or the aforementioned secure data center facilities. Notwithstanding the forgoing, Vendor may retain Protected Information to the extent reasonably necessary to comply with applicable laws and regulations or guidelines provided by an accreditation body (including but not limited to the American National Standards Institute).
DATA ACCURACY INFORMATION	In the event that a parent, student, or eligible student wishes to challenge the accuracy of Protected Information that qualifies as student data for purposes of Education Law, Vendor shall respond to such challenge as required by applicable law.

Dated:______________________________

Michele A. Carpenter	Alsha Gulden 06/17/2024
For the Jefferson-Lewis BOCES	For the Vendor

Attachment B - Parents' Bill of Rights for Data Privacy and Security and BOCES Data Security Policy

Pursuant to New York State Education Law §2-d, parents, legal guardians and persons in parental relation to a student, as well as eligible students, defined as those students who are eighteen years or older, are entitled to certain rights with regard to their child's personally identifiable information (PII), as defined by Education Law §2-d. Jefferson-Lewis BOCES Policy 6001 contains a plain- English summary of such rights. Vendor specifically acknowledges receipt of Parents' Bill of Rights for Data Privacy and Security and BOCES Data Security Policy, which are attached hereto, and understands its legal obligations as provided therein.

[ATTACH POLICIES]

Dated: June 20, 2024

Michele A. Carpenter

For the Jefferson-Lewis BOCES

Alsha Gulden 06/17/2024

For the Vendor

Attachment C – Vendor’s Data Security and Privacy Plan

The BOCES Parents Bill of Rights for Data Privacy Security, receipt of which is acknowledged as Attachment B to this Addendum, is incorporated into and made a part of this Data Security and Privacy Plan.

Privacy Policy: https://www.servsafe.com/Privacy-Policy

Information Security Policy: See attached.

Dated: June 20, 2024

Michele A. Carpenter

For the Jefferson-Lewis BOCES

Alsha Gulden 06/17/2024

For the Vendor

NATIONAL RESTAURANT ASSOCIATION™

Information Security Policy

Information Security Program

Release Date:	4/28/2021	Last Review Date:	9/01/2023
Title:	POL-IT-SEC-001 NRA Information Security Policy		
Version:	1.0	Classification:	**Internal**
Author:	Doug Pedersen, Trustwave	Document Owner:	Sean Kelly
Approved By:	Kevin Steele	Distribution:	INTERNAL USE ONLY

Table of Contents

♦♦ ♦ ♦♦

1 Introduction

1.1 *Purpose*

The National Restaurant Association, an Illinois not-for-profit corporation, together with its wholly-owned subsidiary National Restaurant Association Solutions, LLC, an Illinois limited liability company, and its other affiliated organizations including The National Restaurant Association Educational Foundation, an Illinois not-for-profit corporation (collectively, the "Association").

The purpose of this policy to establish and communicate the Association's expectations for information security within the organization, to ensure the security of sensitive information under the Association's custody or care, and the ongoing secure operation of the organization. Information technologies (IT) are vital to Association operations. They are tools that improve the quality and efficiency of our work and provide the foundation for which our business applications run. They are the repositories for critical and sometimes highly proprietary organizational information. The improper access to or the destruction of these resources will have serious consequences for the Association. It is the purpose of this policy to:

- Ensure organizational IT resources are appropriately protected from destruction, alteration, or unauthorized access.
- Ensure that these protections are accomplished in a manner consistent with the business and workflow requirements of the Association.

1.2 *Scope*

Audience	This policy is applicable to all Association employees, consultants, temporary employees, agents, volunteers and others (collectively, employees) working on any premises of the Association or in a remote location on Association business using Association assets.
Systems	This policy is applicable to all Association assets, systems, networks, and applications.
Locations	This policy is applicable to all Association offices and locations.

1.3 *Responsibilities to this Policy*

The policies contained within this document are under the direction of the Chief Information Officer (CIO) and are to be implemented by all personnel with respect to their use of technology resources. It is each person's responsibility to know and understand the specific directions and actions the organization wants followed.

- The CIO has organizational accountability for the implementation of this policy.
- Every Association employee is responsible for complying with this policy.
- Managers are responsible for ensuring that their staff complies with this policy.
- Managers may include the compromise of the Association information security as part of a performance evaluation.
- Any employee who becomes aware of any violation or suspected violation of this policy must inform the CIO or the Director of Risk, Security, and Compliance (DRSC).

Enforcement and Non-compliance

Compliance issues should be addressed to the Chief Information Officer or the Information Security Council. Where a control cannot be implemented for legitimate business reasons, appropriate compensating controls must be agreed on with Information Security through the exemption process. Violation of this policy may result in the immediate or subsequent revocation or limitation of access to organization information and information assets, as well as disciplinary action, as appropriate, up to and including termination or dismissal.

1.4 *Document Review*

The Information Security Council is responsible for the annual review and subsequent update of the Association's Information Security Policy as well as for the specification of appropriate controls which, when implemented across the business, shall make this policy effective. Recommended changes shall be presented to executive management for approval and then published in a location accessible by all personnel.

1.5 *Revision Log*

Revision #	Date	Description	Revised By
0.1	March 25, 2021	Final Draft	Doug Pedersen, Trustwave (Contributor)

1.5.1 Sign-Off

The signatures below indicate understanding of the materials contained in this document and agreement to the goals, objectives, activities, and responsibilities described herein.

Signature: DocuSigned by: Sean Kelly B86054308F8B44E... Date 6/17/2024

Sean Kelly
Director of Security, Risk and Compliance, National Restaurant Association

Signature: DocuSigned by: Kevin Steele BBE0B9A87DFC4C5... Date 6/17/2024

Kevin Steele
CIO, National Restaurant Association

2 Security Organization Roles & Responsibilities

The proper balance between the leveraging of outsourcing partners and maintaining oversight is based upon an organizational structure which appropriately parses roles and responsibilities among the various outsourced and Organizational components of the IT security organization. The following structure is defined for the Association's security organization:

2.1 *Information Security Council (ISC)*

The Information Security Council is charged with the definition of IT security strategy and scope. The ISC shall be comprised of the:

- Chief Information Officer (CIO)
- Senior Director of Technology
- Director of Security, Risk and Compliance
- Senior Manager of Infrastructure and Support
- Chief Architect
- Director of Software Development

Other participants may, from time to time, include:

- Outsourcing Vendor Project Manager
- Security Advisor

2.2 *Chief Information Officer (CIO)*

Responsible for all NRA Security functions within NRA reporting to the CEO on any matter that has a security component. Sets organization-wide security policies and minimum standards and assesses each business unit on the effective implementation of security controls to comply.

- Reports to executive leadership on all security matters
- Manages overall security risk for all of NRA and business environments
- Directs Governance and Compliance efforts (PCI, CCPA, GDPR, ADA WCAG AA, FERPA)
- Directs Security teams
- Directs Monitoring and Response processes
- Approves exceptions to defined policies and standards

2.3 *Senior Director, Technology Solutions and Operations*

This Organizational function reports to the CIO. Primary responsibility for the oversight of the state of information security at NRA. Primary responsibilities include:

- Leadership of establishing corporate security standards both physical and electronic.
- Owns the policies and minimal standards
- Manages Incident Response Process for all business security incidents
- Manages annual Security Awareness and Incident Response Training programs
- Approval of security policies and procedures.
- Periodic reporting on the state of information security to the CIO.

2.4 *Director, Risk, Security, and Compliance (DRSC)*

Primary liaison between the business unites and the applications and database security efforts. Primary responsibilities include:

- Reporting on the state of information security to the Sr. Director and CIO.
- Drafting and of security policies and procedures.
- Oversight and audit of security efforts accomplished through the IT Audit/Security Coordinator(s).
- Review of applications or database related security policies.
- Recommending and reviewing security strategy through participation in the Information Security Council.
- Oversight of the security efforts of local database administrators, application and database security engineers and other security related specialists as appropriate, insuring adherence to applications or database related security policies.
- Acting as the primary applications and database contact for auditors during a formal audit process.
- Preparation of formal responses and action plans pursuant to internal audits.
- Identification of individuals responsible for security engineering functions in the areas of applications or database administration. These individuals may reside outside of the local NRA environment.

2.5 *Executive Council (EC)*

Top association executives responsible for executing the Association strategic plan. Activities include:

- leading/operating functional segments of the organization,
- strategic planning and
- formulating and enforcing policies focused on meeting association goals

3 Information Security Policies

3.1 *Organization of Information Security*

3.1.1	**Establishment of Security Objectives**
Policy	The Association shall document and maintain policies, procedures and standards to achieve the following security objectives: • To identify and document specific roles and responsibilities to ensure that Information Security is consistently reinforced throughout the Association and that security controls are successfully implemented. • To provide guidance for cooperation with external entities. • To ensure proper authorization for integration of new assets into the Association's environment. • To ensure adequate security of information and information assets when accessed and used by third parties. • To maintain the security of information when outsourced to another organization.
Principle	In order to be effective within an organization, documented policies and controls must be established which, when taken together, provide clear direction to everyone concerning the organization's expectations for information security implementation and provision across the business.
Objective	To provide guidance for documented policies and controls which, when taken together, are: • Up-to-date, suitable and adequate for the Association's business • Provide clear direction to everyone concerning the Association's expectations for information security implementation and provision across the business.
Framework Reference	**NIST CSF:** ID.GV-1 **NIST 800-53r5**: -1 controls from all security control families

3.1.2	**Establish Information Security Policy**
Policy	Documented policies and controls shall be established which, when taken together, provide clear direction to everyone concerning the Association's expectations for information security implementation and provision across the business.
Principle	In order to be effective within an organization, documented policies and controls must be established which, when taken together, provide clear direction to everyone concerning the

	organization's expectations for information security implementation and provision across the business.
Objective	To provide documented policies and controls which, when taken together, are: • Up-to-date, suitable and adequate for the Association's business • Provide clear direction to everyone concerning the Association's expectations for information security implementation and provision across the business.
Framework Reference	**NIST CSF:** ID.GV-1 **NIST 800-53r5**: -1 controls from all security control families

3.1.3 Maintain Information Security Policies

Policy	The Association's information security policies and controls shall be reviewed to ensure their continued suitability, adequacy and effectiveness. This review shall be held: • At planned, regular intervals, but at least annually; • Whenever significant changes to the organization's business, legal, or technical environment occur.
Principle	In order to be effective within an organization, documented policies and controls must be established which, when taken together, provide clear direction to everyone concerning the organization's expectations for information security implementation and provision across the business.
Objective	The Association's information security policies and controls shall be reviewed to ensure their continued suitability, adequacy, and effectiveness.
Framework Reference	**NIST CSF:** ID.GV-1 **NIST 800-53r5**: -1 controls from all security control families

3.1.4 Framework & Taxonomy

Policy	The Association shall establish a framework which shall be used for the management and administration of all information security policies and controls within its business.
Principle	Organizations should implement a framework for the management and administration of their information security policies and controls. This framework should be both simple to comprehend and flexible enough to allow for changes in the future.
Objective	To ensure the effective and consistent management and administration of all information security policies and controls within the Association.
Framework Reference	**NIST CSF:** ID.GV-1 **NIST 800-53r5**: -1 controls from all security control families

3.1.5 Leadership Team Commitment to Information Security

Policy	The Executive Council shall demonstrate its commitment to information security within the Association. This commitment shall be demonstrated by: • Delegating responsibility for the management of information security to the Information Security team • Publishing a high-level statement of support for the implementation of good information security policies and controls within the Association • Allocating appropriate resources • Advocating for Information Security and enforcement of policies
Principle	An organization's commitment to information security must be demonstrated by its Executive Council.
Objective	To make information security effective within the organization.
Framework Reference	**NIST CSF:** ID.BE-3 **NIST 800-53r5:** PM-11

3.1.6 Information Security Organization

Policy	An information Security Council shall be established to lead, manage and co-ordinate the dissemination and implementation of good information security practice.
Principle	In order to be effective within an organization, information security activities must be clearly led, managed and coordinated across the business.
Objective	To provide a focus for the leadership, management, and co-ordination of information security across the business.
Framework Reference	**NIST CSF:** ID.GV-2 **NIST 800-53r5:** PS-7, PS-9, PM-1, PM-2, PM-29

3.1.7 Policy Exceptions

Policy	As necessary, the Association allows for exceptions to the Information Security Policy or subordinate policies, standards, and procedures. Exception requests can be made to the Director of Risk, Security and Compliance and approved by the ISC for up to one year. Exception requests shall list any compensating controls to be put in place to cover the exception.

	Failure to abide by the documented Exception Request is considered a security violation and may be subject to disciplinary action up to and including immediate termination of employment or immediate termination of client, partner, and/or vendor relationship. Exceptions will be logged and reviewed prior to their expiration to ensure that the conditions that created the need for the exception have been resolved.
Principle	In order to be effective within an organization, documented policies and controls must be established which, when taken together, provide clear direction to everyone concerning the organization's expectations for information security implementation and provision across the business.
Objective	To provide documented policies and controls which, when taken together, are: • Up-to-date, suitable and adequate for the Association's business • Provide clear direction to everyone concerning the Association's expectations for information security implementation and provision across the business.
Framework Reference	**NIST CSF:** ID.GV-1 **NIST 800-53r5**: -1 controls from all security control families

3.1.8 External Parties

Policy	Appropriate controls shall be established to maintain the security of the Association's information and information processing facilities that are accessed, processed, communicated to, and/or managed by external parties. Controls put in place shall be in accordance with the Association Third-Party Information Security Risk Management policy.
Principle	An organization must protect its information and information processing facilities that are used by external parties.
Objective	To maintain the security of the Association's information and information processing facilities that are accessed, processed, communicated to, and/or managed by external parties.
Framework Reference	**NIST CSF:** ID.SC-1 **NIST 800-53:** PM-30, SA-9, SR-1, SR-2, SR-3, SR-5

3.1.9 Coordination Between Organizations

Policy	The Association shall maintain appropriate contacts with outside organizations to ensure that appropriate actions can be quickly taken and advice obtained in the event of a security incident. This should include, but is not limited to, the following: • Law enforcement authorities

	• Regulatory agencies • Information service providers • Telecommunications operators • Others, as necessary, to protect the Association's information assets (e.g., Insurance, Legal, Forensics) • Exchanges of security information shall be restricted to ensure that confidential information is not inadvertently provided during a security incident.
Principle	An organization must protect its information and information processing facilities that are used by external parties.
Objective	To maintain the security of the Association's information and information processing facilities that are accessed, processed, communicated to, and/or managed by external parties.
Framework Reference	**NIST CSF:** ID.SC-1 **NIST 800-53:** PM-30, SA-9, SR-1, SR-2, SR-3, SR-5

3.2 *Asset Management*

3.2.1 **Asset Inventory**	
Policy	The Association shall maintain an accurate inventory of all information assets including, but not limited to documentation, hardware and software. This inventory shall include all information necessary to recover from a disaster, including the following: • Asset identification • Hostname • Asset Owner • Asset type • Tenant (where appropriate) • Location • License information • Other information deemed necessary by Association leadership. Each information asset shall have an identified Asset Owner who is accountable for classification of the information asset, responsible for ensuring that the asset is part of documented inventory, and maintenance of related security controls as specified within the ISP.
Principle	An organization must protect its information and information processing assets. In order to do this effectively, an organization must know what its assets are, who owns them and how they should be used to support the business of the organization.

Objective	To achieve and maintain appropriate protection of the Association's information and information processing assets and to ensure that all appropriate licensing requirements are met.
Framework Reference	**NIST CSF:** ID.AM-1; ID.AM-2; ID.AM-4 **NIST 800-53r5:** CM-8, PM-5, AC-20, SA-9

3.2.2 Hardware Inventory

Policy	The Association shall maintain an inventory of all hardware assets, including but not limited to computer equipment, communication equipment, network equipment, magnetic media, and optical media shall be maintained and documented by the identified Asset Owner and shall include a minimum of the following: • Data Owner(s) • Configuration Owner • Host name • IP Address • Dependent Systems (where appropriate) • Associated responsible Operations team • Classification • Device Type • Vendor (where applicable) • Physical location
Principle	An organization must protect its information and information processing assets. In order to do this effectively, an organization must know what its assets are, who owns them and how they should be used to support the business of the organization.
Objective	To achieve and maintain appropriate protection of the Association's information and information processing assets and to ensure that all appropriate licensing requirements are met.
Framework Reference	**NIST CSF:** ID.AM-1; ID.AM-2; ID.AM-4 **NIST 800-53r5:** CM-8, PM-5, AC-20, SA-9

3.2.3 Software Inventory

Policy	An inventory of all software assets including, but not limited to application software, system software, development tools, software utilities, and development code shall be maintained and documented by the identified Data Owner and/or the designated shall include the following: • Information Owner (where appropriate) • Configuration Owner • Dependent Systems (where appropriate)

	• Associated responsible Infrastructure team • Asset Classification • Vendor (where applicable) • Software license (where applicable) term
Principle	An organization must protect its information and information processing assets. In order to do this effectively, an organization must know what its assets are, who owns them and how they should be used to support the business of the organization.
Objective	To achieve and maintain appropriate protection of the Association's information and information processing assets and to ensure that all appropriate licensing requirements are met.
Framework Reference	**NIST CSF:** ID.AM-1; ID.AM-2; ID.AM-4 **NIST 800-53r5:** CM-8, PM-5, AC-20, SA-9

3.2.4 Data Classification

Policy	An appropriate data classification scheme shall be established and implemented across the whole of the Association that considers the data's value, sensitivity, and criticality to the Association's business. This scheme shall be detailed in the NRA Data Classification and Handling Policy.
Principle	An information classification scheme should be established that applies throughout the organization, based on the confidentiality of the information in use.
Objective	To ensure that all of the Association's data receives an appropriate level of protection thereby preventing unauthorized disclosure.
Framework Reference	**NIST CSF:** ID.AM-5 **NIST 800-53r5:** CP-2, RA-2, RA-9, SA-20, SC-6

3.2.5 New Assets

Policy	The acquisition and use of any new information assets shall have appropriate managerial approval. Prior to implementation or integration into any environment, all hardware/software assets shall be evaluated for to ensure compliance with and support for business and security requirements.
Principle	An organization must protect its information and information processing assets. In order to do this effectively, an organization must know what its assets are, who owns them and how they should be used to support the business of the organization.
Objective	To achieve and maintain appropriate protection of the Association's information and information processing assets and to ensure that all appropriate licensing requirements are met.

Framework Reference	**NIST CSF:** PR.IP-2; PR.DS-4 **NIST 800-53r5:** SA-3, SA-4, SA-8, SA-10, SA-11, AU-4, CP-2, PE-11, SC-5

3.3 *Risk Management*

	3.3.1 **Information Risk Management**
Policy	Risks to the Association's information assets shall be assessed and managed on a continual and regular basis.
Principle	In order to protect its information assets effectively, an organization must continually make an assessment of the risks to those assets and must establish an active program to manage those risks. Risks to an organization's information assets may arise from: • external threats • internal vulnerabilities.
Objective	To ensure that the risks to the Association's information assets are assessed and managed effectively, and to ensure that these risks are considered and afforded a priority in all the decision-making processes across the business.
Framework Reference	**NIST CSF:** ID.GV-4; ID.RA-1:6; ID.RM-1:3 **NIST 800-53r5:** PM-3, PM-4, PM-7, PM-9, PM-10, PM-11, PM-12, PM-15, PM-16, PM-28, RA-1, RA-2, RA-3, RA-5, RA-7, RA-9, RA-10, CA-2, CA-5, CA-7, CA-8, CP-2, SA-2, SA-5, SA-11, SI-2, SI-4, SI-5

	3.3.2 **Risk Register**
Policy	The Association shall develop a Risk Register to be used to log risks identified through the risk assessment process. The risk register shall include at least: • Risk Name • A Unique Risk Identifier (serial number or code) • Who Identified the Risk • Association Systems/Assets Potentially Impacted • Risk Description • Risk Category (Internal vs External) • Risk Cause (what event would trigger the risk) • Risk Result (impact to the Association if risk happens) • Date Risk was Identified

	• Initial Impact • Initial Likelihood • Risk (Initial Impact x Initial Likelihood) • Risk Owner • Risk Mitigation Plan • Risk Mitigation Cost • Residual Impact • Residual Likelihood • Residual Risk (Residual Risk x Residual Impact)
Principle	In order to protect its information assets effectively, an organization must continually make an assessment of the risks to those assets and must establish an active program to manage those risks. Risks to an organization's information assets may arise from: • external threats • internal vulnerabilities.
Objective	To ensure that the risks to the Association's information assets are assessed and managed effectively, and to ensure that these risks are considered and afforded a priority in all the decision-making processes across the business.
Framework Reference	**NIST CSF:** ID.GV-4; ID.RA-1:6; ID.RM-1:3 **NIST 800-53r5:** PM-3, PM-4, PM-7, PM-9, PM-10, PM-11, PM-12, PM-15, PM-16, PM-28, RA-1, RA-2, RA-3, RA-5, RA-7, RA-9, RA-10, CA-2, CA-5, CA-7, CA-8, CP-2, SA-2, SA-5, SA-11, SI-2, SI-4, SI-5

3.3.3 Risk Review and Update

Policy	The Association shall review and update the Risk Register at least quarterly.
Principle	In order to protect its information assets effectively, an organization must continually make an assessment of the risks to those assets and must establish an active program to manage those risks. Risks to an organization's information assets may arise from: • external threats • internal vulnerabilities.
Objective	To ensure that the risks to the Association's information assets are assessed and managed effectively, and to ensure that these risks are considered and afforded a priority in all the decision-making processes across the business.
Framework Reference	**NIST CSF:** ID.GV-4; ID.RA-1:6; ID.RM-1:3 **NIST 800-53r5:** PM-3, PM-4, PM-7, PM-9, PM-10, PM-11, PM-12, PM-15, PM-16, PM-28, RA-1, RA-2, RA-3, RA-5, RA-7, RA-9, RA-10, CA-2, CA-5, CA-7, CA-8, CP-2, SA-2, SA-5, SA-11, SI-2, SI-4, SI-5

3.3.4 Risk Management Reporting

Policy	Risks to the Association's information assets shall be compiled and reported to the Association ISC quarterly and Executive Council on at least an annual basis.
Principle	In order to protect its information assets effectively, an organization must continually make an assessment of the risks to those assets and must establish an active program to manage those risks. Risks to an organization's information assets may arise from: • external threats • internal vulnerabilities.
Objective	To ensure that the risks to the Association's information assets are assessed and managed effectively, and to ensure that these risks are considered and afforded a priority in all the decision-making processes across the business.
Framework Reference	**NIST CSF:** ID.GV-4; ID.RA-1:6; ID.RM-1:3 **NIST 800-53r5:** PM-3, PM-4, PM-7, PM-9, PM-10, PM-11, PM-12, PM-15, PM-16, PM-28, RA-1, RA-2, RA-3, RA-5, RA-7, RA-9, RA-10, CA-2, CA-5, CA-7, CA-8, CP-2, SA-2, SA-5, SA-11, SI-2, SI-4, SI-5

3.3.5 Threat Intelligence

Policy	The Association shall: • Collect cyber -threat intelligence through membership in information sharing forums that discuss cyber security risks and threats, • Subscribe to threat-intelligence feeds from vendors • Generate and disseminate internal security alerts, advisories, and notices to IT and general users as applicable.
Principle	In order to protect its information assets effectively, an organization must continually make an assessment of the risks to those assets and must establish an active program to manage those risks. Risks to an organization's information assets may arise from: • external threats • internal vulnerabilities.
Objective	To ensure that the risks to the Association's information assets are assessed and managed effectively, and to ensure that these risks are considered and afforded a priority in all the decision-making processes across the business.
Framework Reference	**NIST CSF:** ID.RA-2 **NIST 800-53r5:** PM-15, PM-16, RA-10, SI-5

3.4 *Personnel Security*

3.4.1 **Personnel Security Prior to Employment**	
Policy	Appropriate consideration shall be given to information security matters throughout the recruitment process. The Association People + Culture team shall document standards for "passing" criminal background checks (i.e. what background findings are grounds for not hiring) and credit checks (i.e. what is the minimum credit score acceptable). The Association employee candidates People + Culture team shall successfully pass a criminal background and credit checks administered by the Association People + Culture team before employees are provided access to the Association systems.
Principle	Information security matters should be embedded throughout all personnel processes, especially the recruitment process. Appropriate common processes should be established that apply throughout the organization.
Objective	To ensure that all employees, contractors and third-party users understand their responsibilities and are suitable for the roles for which they are considered, and to reduce the risk of theft, fraud, or misuse of facilities.
Framework Reference	**NIST CSF** : PR.IP-11 **NIST 800-53r5:** PS-1, PS-2, PS-3, PS-4, PS-5, PS-6, PS-7, PS-8, PS-9, SA-21

3.4.2 **Personnel Security During Employment**	
Policy	Appropriate consideration shall be given to information security matters throughout the employment process. The Association shall document: • All job role definitions shall include appropriate language identifying the correlating Information Security responsibilities for said job role. • Management shall be responsible for working with the Culture & People Experience team and Security to identify job role specific security concerns for job roles. • All employees, who are given access to Association owned or managed information assets, shall sign the Association's confidentiality or non-disclosure agreement prior to being granted access to any Association owned or managed information asset. • All employees shall be responsible for working with the Association's identified security teams to support the implementation of a corporate-wide security environment. • Full compliance with the ISP is a condition of employment. Violation of the ISP may result in disciplinary action up to and including immediate termination.

Principle	Information security matters should be embedded throughout all personnel processes, especially the employment process. An appropriate common employment process should be established that applies throughout the organization.
Objective	To ensure that all employees, contractors and third-party users are aware of information security threats and concerns, their responsibilities and liabilities.
Framework Reference	**NIST CSF:** PR.IP-11 **NIST 800-53r5:** PS-1, PS-2, PS-3, PS-4, PS-5, PS-6, PS-7, PS-8, PS-9, SA-21

3.4.3 Personnel Security on Termination or Change of Employment

Policy	Appropriate consideration shall be given to information security matters throughout the termination or change of employment process. On notice of change of employment, the Association shall: • Disable information system access the same day the user is no longer an Association employee. • Terminates/revokes any authenticators/credentials associated with the employee; • Retrieves all Association assets and any security-related organizational information system-related property; • Retains access to organizational information and information systems formerly controlled by employee; and • Notify IT Personnel that the employee is no longer in the employ of the Association.
Principle	Information security matters should be embedded throughout all personnel processes, especially the termination or change of employment process. An appropriate common process should be established that applies throughout the organization.
Objective	To ensure that all employees, contractors and third-party users exit an organization or change employment in an orderly manner.
Framework Reference	**NIST CSF:** PR.IP-11 **NIST 800-53r5:** PS-1, PS-2, PS-3, PS-4, PS-5, PS-6, PS-7, PS-8, PS-9, SA-21

3.5 *Awareness & Training*

3.5.1 Information Security Awareness and Training

Policy	A comprehensive information security awareness and training program shall be established and rolled-out across the whole of the Association in order to ensure that all the Association's employees,

	and where relevant, contractors and third-party users are made aware of the risks and issues associated with the protection of its information assets and information processing systems. • All new Association employees are granted access to the Association's information resources to facilitate completion of new hire training curriculum, which includes required security awareness training. New hire security awareness training must be completed within ten (10) business days of start date. • All employees shall be required to complete security awareness training at least annually, to ensure that all personnel are aware of the importance of Information Security. • Failure to complete the Association's mandatory security awareness training will be deemed a violation of the Employee Standards of Conduct, which may result in disciplinary action up to and including termination of employment. • Security shall be responsible for working with training organizations, legal and compliance teams to develop relevant security training material.
Principle	One of the most cost-effective ways in which an organization can reduce the risk of information security breaches is to ensure that its employees are made aware of the risks and issues associated with the protection of its information assets and information processing systems. This is best achieved by means of a coordinated and consistent program of information security awareness which reaches every part of the business. Further reductions in risk can be made by including contractors and third-party users in this awareness program.
Objective	To ensure that all Association employees and, where relevant, contractors and third-party users are aware of information security issues relevant to their job and to remind them of their responsibilities and liabilities in this regard.
Framework Reference	**NIST CSF:** PR.AT-1:5 **NIST 800-53r5:** AT-2, AT-3, PM-13, PM-14, PS-7, SA-9, CP-3, IR-2

3.6 *Physical & Environmental Security*

3.6.1	**Secure Areas**
Policy	Critical and sensitive business information processing facilities shall be housed in secure areas and protected by a defined security perimeter, with appropriate security barriers and entry controls. Access to these areas shall be limited to Association personnel with job duties that require physical access to information processing facilities. Lists of Association employees with access to these facilities shall be automatically maintained, and reviewed at least annually.

Principle	Organizations should ensure the physical security of their critical and sensitive business processing facilities. These facilities should be physically protected from unauthorized access, damage and interference. The protection provided should be commensurate with the risks identified.
Objective	To prevent unauthorized physical access, damage and interference to the organization's premises and information.
Framework Reference	**NIST CSF:** PR.AC-2 **NIST 800-53r5:** PE-1, PE-2, PE-3, PE-4, PE-5, PE-6, PE-8, PE-9

3.6.2 Equipment Security

Policy	Appropriate controls shall be established to protect all equipment that is used to support the Association's business activities.
Principle	An organization's equipment should be physically protected from threats and environmental hazards. Protection of equipment is necessary in order to reduce the risk of unauthorized access to information and to protect against loss or damage of the equipment itself.
Objective	To prevent loss, damage, theft or compromise of assets and the interruption of the Association's business activities.
Framework Reference	**NIST CSF:** PR.IP-5 **NIST 800-53r5:** PE-1

3.7 *Security Operations*

3.7.1 Operational Procedures and Responsibilities

Policy	Responsibilities and procedures for the management and operation of all information processing facilities shall be established.
Principle	In order for an organization's information systems to support the business effectively and efficiently, their day-to-day operation should be well managed and controlled. This should include: the specification of well-defined responsibilities, the establishment of appropriate operating instructions and the segregation of duties.
Objective	To ensure the correct and secure operation of information processing facilities.
Framework Reference	**NIST CSF:** ID.GV-2 **NIST 800-53r5:** PS-7, PS-9, PM-1, PM-2, PM-29

3.7.2 Third Party Services Delivery Management

Policy	Services delivered by third parties shall be given an appropriate level of protection commensurate with the risks to those services.
Principle	Organizations that employ third party services should ensure that an appropriate level of protection is established by the third party for the information and other service deliverables that it supplies.
Objective	To implement and maintain the appropriate level of information security and service delivery in line with third party service delivery agreements.
Framework Reference	**NIST CSF:** ID.SC-3 **NIST 800-53r5:** SA-4, SA-9, SR-2, SR-3, SR-5

3.7.3 Backups

Policy	Procedures shall be established for the carrying out of an agreed back-up strategy and which shall include taking back-up copies of data and rehearsing their timely restoration, logging events and faults and, where appropriate, monitoring the equipment environment. • Backup copies of essential the Association business information and software shall be taken on a regular basis. • Adequate backup facilities shall be provided to ensure that all essential the Association business information and software can be recovered following a disaster or media failure. • Backup arrangements for individual systems shall be regularly tested to ensure that they meet the requirements of the Association Business Continuity/Disaster Recovery (BC/DR) plans. • A minimum level of backup information, together with accurate and complete records of the backup copies and documented restoration procedures, shall be stored in a remote location at a sufficient distance to escape any damage from a disaster at the main site. • Backup information shall be given the appropriate level of physical and environmental protections. • Backup media shall be regularly tested, where practical, to ensure the media can be relied upon for emergency use when necessary. • Restoration procedures shall be regularly checked and tested to ensure they are effective and they can be completed within the time allotted. • Retention and archive standards shall be followed as specified in the NRA Media and Records Retention Standard.
Principle	In order to ensure that their business is able to be maintained in the face of a disruption or a disaster, organizations should develop and implement a comprehensive back-up strategy and ensure that it is implemented effectively.

Objective	To maintain the integrity and availability of information and information processing facilities.
Framework Reference	**NIST CSF:** PR.IP-4; PR.PT-5 **NIST 800-53r5:** CP-4, CP-6, CP-7, CP-8, CP-9, CP-11, CP-12, CP-13, PE-11, PL-8, SC-6

3.7.4 Media Handling

Policy	Appropriate operating procedures shall be established to protect documents, computer media (tapes, disks), input / output information and systems documentation from damage, theft and unauthorized access. • The Association prohibits the use of writeable removable media in Association workstations. • Removable media includes but is not limited to: writable optical media, external portable storage devices, flash memory devices, MP3 Players, Tablets, PDAs, mobile phones, etc. • Employees will be permitted to use writeable removable media when the frequent use of such is required by their specific job responsibilities. All such cases must be individually documented and approved by a senior manager and Security through the ISP Exception Request Process. • Media shall be disposed of securely and safely when no longer required for business processes in accordance with the NRA Data Classification and Handling Policy and the NRA Media Disposal standard.
Principle	Organizations should protect its information in all the various forms that it exists, both paper and electronic.
Objective	To prevent unauthorized disclosure, modification, removal, or destruction of assets and interruption to the Association's business activities.
Framework Reference	**NIST CSF:** PR.PT-2; PR.DS-3 **NIST 800-53r5:** MP-1, MP-2, MP-3, MP-4, MP-5, MP-6, MP-7, MP-8, CM-8, PE-16, PE-20

3.7.5 Exchange of Information

Policy	Exchanges of information and software between the Association and other organizations shall be controlled and shall be compliant with all relevant legislation.
Principle	Organizations that wish to establish business arrangements to exchange information and software should do so in a formally agreed and controlled manner. Procedures to protect information and media in transit should be established. Business and information security implications associated with electronic data interchange, electronic commerce and electronic mail should be considered.

Objective	To maintain the security of information and software exchanged within an organization and with any external entity.
Framework Reference	**NIST CSF:** ID.AM-3; PR.DS-2 **NIST 800-53r5:** AC-4, CA-3, CA-9, PL-8, SA-17, SC-8, SC-11

3.7.6 Logging and Monitoring

Policy	The Association shall define and implement standards and their associated procedures to create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.
Principle	Organizations should be watchful that their information processing facilities are only being used for legitimate and authorized purposes.
Objective	To detect unauthorized and malicious activities in the Association environment.
Framework Reference	**NIST CSF:** DE.AE-1:5; DE.CM-1:8; DE.DP-1:5 **NIST 800-53r5:** all -1 controls, AC-2, AC-4, AU-6, AU-12, AU-13, CA-1, CA-2, CA-3, CA-7, CM-2, CM-3, CM-8, CM-10, CM-11, CP-2, IR-4, IR-5, IR-8, RA-3, RA-5, PE-6, PE-20, PM-14, SA-4, SA-9, SI-1, SI-3, SI-4, SI-8, SC-5, SC-7, SC-16, SC-18, SC-44, SR-1, SR-9, SR-10, PL-2, PS-7

3.7.7 Cloud Computing

Policy	Appropriate controls shall be established to maintain the security of the Association's information and information processing environments that are located in or supported by Cloud Computing services.
Principle	Organizations should protect their sensitive information when it is stored, processed or transmitted by means of Cloud Computing services.
Objective	To protect sensitive information which is stored, processed, or transmitted by means of Cloud Computing services.
Framework Reference	**NIST CSF:** PR.AC-5; PR.IP-1 **NIST 800-53r5:** AC-4, AC-10, SC-7, SC-10, SC-20, CM-1, CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10

3.8 *Protection Against Malicious Software*

3.8.1	**Protection Against Malicious and Mobile Code**
Policy	The Association shall implement measures to prevent and detect the introduction of malicious software in its networks and information processing facilities. Non-Association equipment that connects to Association resources shall be subject to the same patch and endpoint (e.g., laptop, desktop, server, and other mobile and network devices or software) protection requirements as Association owned or managed equipment.
Principle	Software and information processing facilities are vulnerable to the introduction of malicious software such as: computer viruses, network worms, Trojan horses and logic bombs (this list is not exhaustive). Organizations need to implement precautions to detect such malicious software and to protect against it.
Objective	To protect the integrity of the Association's software and information.
Framework Reference	**NIST CSF:** DE.CM-4:5 **NIST 800-53r5:** SI-3, SI-4, SI-8, SC-18, SC-44

3.8.2	**Vulnerability Management**
Policy	Vulnerability management is a necessary part of the overall security framework at the Association. For the purposes of the ISP, the Association defines a vulnerability detection solution as the automated process of proactively identifying vulnerabilities of computing systems in a network in order to determine if and where a system can be exploited or threatened. the Association considers vulnerability detection to be a part of a secured operating infrastructure, and as such, the following shall be adhered to: • The Association shall maintain centrally supported and administered vulnerability detection solutions. All network connected systems, and devices must participate in the Association's corporate vulnerability detection solution. • Third parties are prohibited from conducting vulnerability assessment activities except when explicitly approved by Security. • The Association Security Team shall maintain overall responsibility for setup, administration, and maintenance of all centrally managed vulnerability detection systems deployed at Association locations. • Centrally managed vulnerability detection systems shall be updated on a regular basis. o This regular basis shall be no less than once a month, or as new updates are available. • Exception requests for a vulnerability detection scan shall be temporary. o All granted exception requests shall be based on the fact that the team requesting the exception will resolve all issues by a stated date. • The Asset Owner will review, approve, and oversee exceptions relevant to the environments for which they are responsible.

Principle	Software and information processing facilities are vulnerable to the introduction of malicious software such as: computer viruses, network worms, Trojan horses and logic bombs (this list is not exhaustive). Organizations need to implement precautions to detect such malicious software and to protect against it.
Objective	To protect the integrity of the Association's software and information.
Framework Reference	**NIST CSF:** DE.CM-4:5 **NIST 800-53r5:** SI-3, SI-4, SI-8, SC-18, SC-44

3.8.3 Configuration and Patch Management

Policy	All Association-owned or managed devices shall be periodically updated with vendor patches and system upgrades, where applicable. • Appropriate testing of patches/upgrades and change management procedures shall be followed for all applied patches and upgrades. • All Association owned IT assets will be configured in a secure manner, centrally managed, and take advantage of the latest technology for implementing secure configurations. • Systems classified as "RESTRICTED" shall follow an industry accepted hardening procedure, such as the benchmarks provided by the Center for Internet Security (CIS). • In order to protect the Association's environment, failure to patch or update systems in a timely manner may result in removal of a system from the Association's network without notification.
Principle	Software and information processing facilities are vulnerable to the introduction of malicious software such as: computer viruses, network worms, Trojan horses and logic bombs (this list is not exhaustive). Organizations need to implement precautions to detect such malicious software and to protect against it.
Objective	To protect the integrity of the Association's software and information.
Framework Reference	**NIST CSF:** DE.CM-4:5 **NIST 800-53r5:** SI-3, SI-4, SI-8, SC-18, SC-44

3.8.4 Intrusion Detection Systems (IDS)/Intrusion Prevention Systems (IPS)

Policy	The Association IT department will maintain a duty to protect the Association assets from exploitation of vulnerabilities by ensuring all detection solutions take advantage of the latest technology and offer multiple layers of detection.

	- All critical Association systems and devices, or those deemed necessary by the Association, shall be monitored by a centrally managed IDS/IPS solution. - Management of the Association's IDS/IPS solution shall be maintained by the Information Security Team. - Asset Owners shall be responsible for ensuring that devices within their realm of responsibility, which are considered the Association core business critical, participate in the Association's IDS/IPS solution. - IDS/IPS solutions shall be implemented and maintained to the minimum industry standard expectation.
Principle	Software and information processing facilities are vulnerable to the introduction of malicious software such as: computer viruses, network worms, Trojan horses and logic bombs (this list is not exhaustive). Organizations need to implement precautions to detect such malicious software and to protect against it.
Objective	To protect the integrity of the Association's software and information.
Framework Reference	**NIST CSF:** DE.CM-4:5 **NIST 800-53r5:** SI-3, SI-4, SI-8, SC-18, SC-44

3.9 *Access Control*

3.9.1	**Business Requirement for Access Control**
Policy	The Association shall implement effective access controls, as defined in the NRA Identity & Access Management Policy, which shall allow access to its information and information processing facilities by authorized users for legitimate business reasons only.
Principle	Organizations should protect their information and information processing facilities by ensuring that only those with a legitimate business need can access them.
Objective	To control access to information through alignment to business defined requirements.
Framework Reference	**NIST CSF:** PR.AC-1; PR.AC-4 **NIST 800-53r5:** IA-1, IA-2, IA-3, IA-4, IA-5, IA-7, IA-8, IA-9, IA-10, IA-11, IA-12, AC-1, AC-2, AC-3, AC-5, AC-6, AC-14, AC-16, AC-24

3.9.2 Identity Management

Policy	Formal authorization processes shall be established to control the allocation of access rights to the Association's information systems and services and to implement the principle of least privilege for user and system accounts. The operation of certain duties shall be separated to reduce the opportunities for single individuals to misuse information or services. These duties will be listed in the NRA Identity Management Standard.
Principle	All access to an organization's information and to its information systems should be controlled through a formal authorization process.
Objective	To ensure authorized user access and to prevent unauthorized access to information systems. To ensure clear segregation of duties where required. To limit the risks presented by generic accounts.
Framework Reference	**NIST CSF:** PR.AC-1; PR.AC-4; PR.AC-6 **NIST 800-53r5:** AC-1, AC-2, AC-3, AC-5, AC-6, AC-14, AC-16, AC-24, IA-1, IA-2, IA-3, IA-4, IA-5, IA-7, IA-8, IA-9, IA-10, IA-11, IA-12, PE-2, PS-3

3.9.3 User Responsibilities

Policy	Users shall be made aware of their responsibilities for maintaining effective access controls, particularly regarding the use of passwords and the security of user equipment.
Principle	Organizations should make the first line of defense for their information systems, as strong as possible. This must be achieved within practical limits, to protect data, applications, systems and infrastructure items against unauthorized access. This first line of defense is normally achieved by use of User IDs and their associated passwords. The co-operation of authorized users is essential for effective information security.
Objective	To ensure user accountability for safeguarding their authentication information and to prevent unauthorized user access to the information processing environment and compromise or theft of information.
Framework Reference	**NIST CSF:** PR. AT-1 **NIST 800-53r5:** AT-2, PM-13, PM-14

3.9.4 Operating System, Application, and Database Access Control

Policy	Access to and the administration of all operating system platforms, applications, and databases in the Association shall be strictly managed and controlled.

Principle	Business processing facilities rely upon the integrity of the operating system platforms on which they are hosted and the databases that they use. Organizations should protect the integrity of the operating system platforms and databases that it deploys and should protect access to their information which is held in applications by the implementation of strict access controls.
Objective	To prevent unauthorized access to operating system platforms, applications, and databases.
Framework Reference	**NIST CSF:** PR.AC-1; PR.AC-3:5; PR.AC-7 **NIST 800-53r5:** IA-1, IA-2, IA-3, IA-4, IA-5, IA-7, IA-8, IA-9, IA-10, IA-11, IA-12, AC-1, AC-2, AC-3, AC-4, AC-5, AC-6, AC-10, AC-14, AC-16, AC-17, AC-19, AC-20, AC-24, SC-7, SC-10, SC-15, SC-20

3.9.5 Network Access Control

Policy	Appropriate measures shall be implemented to ensure that users who have access to networks and network services are authorized to do so and do not compromise the security of these networks.
Principle	Organizations should control access to their internal and external networked services.
Objective	To prevent unauthorized access to network services.
Framework Reference	**NIST CSF:** PR.AC-4; PR.AC-7 **NIST 800-53r5:** AC-1, AC-2, AC-3, AC-5, AC-6, AC-14, AC-16, AC-24, IA-1, IA-2, IA-3, IA-5, IA-8, IA-9, IA-10, IA-11

3.9.6 Mobile Computing and Remote Access

Policy	Unauthorized network devices, such as modems or Wireless Access Points, shall not be connected to PCs, workstations, or laptops. The following restrictions are in place: • The use of devices and software that permits remote access to Association workstations from anywhere except from Association systems located on the internal Association network is prohibited. • Remotely connecting to Association owned devices from home computers or non-Association owned devices using unapproved methods is prohibited. • Remote access to the Association's network, or any device contained on the Association's network shall be provided through a secured system or through a VPN connection and shall require at least two-factor authentication. • Remote access connections to the Association's network or individual network devices which do not pass through approved firewalls or secure authentication servers shall be strictly prohibited and, prior to implementation or use, shall require approval from Security through the ISP Exception Request Process.

	• Auditing and logging of significant events shall be enabled, stored centrally by Security, and monitored for all remote access connections.
Principle	Organizations should ensure that the risks of mobile computing and remote access for its staff are understood and addressed in an appropriate manner.
Objective	To ensure that authorized users of organizational computer systems connect to those systems, networks, and data repositories to conduct organization-related business through secure, authenticated and carefully managed business approved access methods.
Framework Reference	**NIST CSF:** PR.AC-3 **NIST 800-53r5**: AC-1, AC-17, AC-19, AC-20, SC-15

3.9.7 Wi-Fi Networks and Devices

Policy	• The Association prohibits the operation of Wi-Fi networks and devices that have not been approved or implemented by the Association. This includes implementation at any location or facility managed, owned or leased by the Association. • All Wi-Fi networks and associated configurations shall be reviewed and approved by the Association Security. • Security or designee shall be authorized to use scanners and other similar tools to monitor for rogue access points, networks, and other wireless devices. Wireless Intrusion Detection/Prevention and other monitoring tools shall be implemented. • Any unauthorized device detected by scanning or identified through physical means as being used while on Association premises shall be deactivated and can be removed or confiscated by an authorized security administrator. • All employee users connecting to Wi-Fi networks must be authenticated and the ability to track each device to a user must be maintained. • Individuals who are not Association employees or third-party contractors shall not be permitted to access the Association Production Wi-Fi networks. • All approved device configurations will be reviewed by Security teams on a periodic basis to maintain adherence to industry accepted practices. • All access to such Wi-Fi networks must be validated by at least two-factor authentication methods. • The strongest industry standard Wi-Fi authentication and encryption protocols must be used at all times. Devices and networks that cannot are not permitted.
Principle	Organizations should ensure that the risks of mobile computing and remote access for its staff are understood and addressed in an appropriate manner.
Objective	To ensure that authorized users of organizational computer systems connect to those systems, networks, and data repositories to conduct organization-related business through secure, authenticated and carefully managed business approved access methods.

Framework Reference	**NIST CSF:** PR.AC-3 **NIST 800-53r5**: AC-1, AC-17, AC-19, AC-20, SC-15

3.9.8 Guest Wi-Fi Networks

Policy	Where it is deemed appropriate by the Association management, the Association Operations teams may deploy secured Wi-Fi networks for guest access to the internet. Such networks must always be configured and managed to current industry accepted practices and must at a minimum meet the following requirements: • Unless prohibited by job function, duties, or contractual/regulatory requirements all Association employees with a valid and functional Association Active Directory account shall be permitted to use these approved networks. • Devices permitted to access such networks must be identifiable to the individual owner. • The strongest industry standard Wi-Fi authentication and encryption protocols must be used at all times. Devices and networks that cannot are not permitted. • Guest networks may never allow direct connectivity to the Association's internal networks.
Principle	Organizations should ensure that the risks of mobile computing and remote access for its staff are understood and addressed in an appropriate manner.
Objective	To ensure that authorized users of organizational computer systems connect to those systems, networks, and data repositories to conduct organization-related business through secure, authenticated and carefully managed business approved access methods.
Framework Reference	**NIST CSF:** PR.AC-3 **NIST 800-53r5**: AC-1, AC-17, AC-19, AC-20, SC-15

3.9.9 Authorized Use Banner

Policy	The following banner, or similar language, shall be displayed wherever user logon occurs for the Association assets: This system is for authorized use only. Any use of the system is subject to monitoring and recording by systems personnel. Anyone using this system expressly consents to such monitoring and recording and is advised that if such monitoring and/or recording reveals possible criminal or unethical activity, system personnel may, in addition to other actions, provide the evidence of such monitoring to law enforcement officials.
Principle	Business processing facilities rely upon the integrity of the operating system platforms on which they are hosted and the databases that they use. Organizations should protect the integrity of the

	operating system platforms and databases that it deploys and should protect access to their information which is held in applications by the implementation of strict access controls.
Objective	To prevent unauthorized access to operating system platforms, applications, and databases.
Framework Reference	**NIST CSF:** PR.AC-1; PR.AC-3:5; PR.AC-7 **NIST 800-53r5:** IA-1, IA-2, IA-3, IA-4, IA-5, IA-7, IA-8, IA-9, IA-10, IA-11, IA-12, AC-1, AC-2, AC-3, AC-4, AC-5, AC-6, AC-10, AC-14, AC-16, AC-17, AC-19, AC-20, AC-24, SC-7, SC-10, SC-15, SC-20

3.10 *Network and Communications*

3.10.1	**Network Security Management**
Policy	Appropriate measures shall be implemented to ensure the effective security management of Association networks. • Access to the Association's network infrastructure shall be explicitly denied unless specifically authorized. • All Association clients shall be segmented by stateful inspection firewalls and only the services required to conduct the Association business and support permitted in and out of client environments. • All software installed on network-attached devices shall be maintained at a level supported by the vendor. • Operational responsibility for network assets shall be separated from network security operations where appropriate. • Personnel responsible for the management of network components must have defined roles and responsibilities. All personnel must be made aware of the responsibility of securing network components. • Security will maintain oversight of the secure operation of all network devices. • All assets connected to the Association's network shall have an identified and documented Information Custodian (see NRA Data Classification and Handling Policy). • Information Custodians responsible for network assets shall implement and maintain necessary security controls for the Association's network assets. • Where necessary and required by regulatory or contractual requirements, special controls shall be implemented to safeguard the confidentiality and integrity of data passing over public networks. • Network and network-related asset design, implementation, administration, maintenance and decommission shall take security into consideration during all phases of each network asset life cycle. • Detailed information related to the Association's network shall be classified as INTERNAL USE ONLY. • Access to or disclosure of network-related information shall be strictly prohibited and shall require appropriate authorization prior to disclosure.

	• All information assets used to manage, pass or filter network traffic shall be maintained within an appropriate physically secured location. • Firewalls, demilitarized zones (DMZs) and proxy servers shall be implemented where necessary or appropriate to protect Association business processes. • All users shall be required to authenticate themselves at a firewall prior to establishing a real time connection with any Association internal information asset over the Internet. • With the exception of telecommuters and mobile computer users, all users shall be required to authenticate to the Internet through Association proxy servers. • All users shall be prohibited from establishing Internet or other external network connections to the Association’s internal network, which could allow a non-Association user access to Association systems. • New and existing internet connections shall be used only for Association sanctioned business activities. • The use of remote control software shall be strictly prohibited, and shall be prohibited from connecting into the Association’s network or to the Association’s network assets from a public network without approval from Security through the ISP Exception Request Process. • Standard Microsoft and Mac desktop firewall software shall be installed and active on all Association owned or managed workstations (e.g., desktops and laptops).
Principle	Organizations should implement a range of controls to ensure the effective security management of their networks which may cross organizational boundaries.
Objective	To ensure the protection of information in networks and the protection of the supporting infrastructure.
Framework Reference	**NIST CSF:** PR.AC-5 **NIST 800-53r5:** AC-4, AC-10, SC-7, SC-10, SC-20

3.10.2 Network Encryption

Policy	Information shall be encrypted during transmission in accordance with the NRA Data Classification and Handling Policy and the NRA Encryption Policy.
Principle	Organizations should protect their sensitive information via cryptographic means when it is transmitted over open, public networks.
Objective	To protect sensitive information that is transmitted over open, public networks.
Framework Reference	**NIST CSF:** PR.DS-2 **NIST 800-53r5:** SC-8, SC-11

3.10.3 Network Management

Policy	Appropriate measures shall be implemented to ensure the effective management of the Association's networks. • An asset management process shall be in place that ensures an inventory of network devices is maintained that includes, at a minimum, IP subnet designation, hostnames, asset owner, and other relevant information. • Traffic present on the Association's network shall be restricted and shall originate or terminate on assets that are authorized to be on the Association's network. • Asset Owners are responsible for network assets and shall work with appropriate teams to document relevant operational procedures for all network assets. • Network device audit logs shall be enabled and stored in a centrally managed log management solution and reviewed and/or monitored by the Association. • Network assets shall be, at a minimum, maintained to applicable industry standards. • Network diagrams must be kept current and describe how networks are configured as well as identify the location of all network devices.
Principle	Organizations should implement a range of controls to ensure the effective management of their networks which may cross organizational boundaries.
Objective	To protect sensitive information that is transmitted over open, public networks.
Framework Reference	**NIST CSF:** PR.AC-5 **NIST 800-53r5:** AC-4, AC-10, SC-7, SC-10, SC-20

3.10.4 Security Requirements for Information Systems

Policy	Information security requirements shall be identified, agreed and documented prior to the development of any information system or application.
Principle	All information security requirements, including the need for fallback activities, should be identified at the requirements phase of a project and justified, agreed and documented as part of the overall business case for an information system.
Objective	To ensure that security is an integral part of information systems.
Framework Reference	**NIST CSF:** PR.IP-2 **NIST 800-53r5:** SA-3, SA-4, SA-8, SA-10, SA-11

3.11 *Systems Development*

3.11.1 Correct Processing in Applications

Policy	Appropriate functions to support the integrity of processing, shall be designed into business applications. Such functions shall include, but shall not be restricted to: • Validation of input data • Validation of internal processing • Validation of output data • Event and audit logging
Principle	Organizations should ensure that their business applications enforce correct processing which ensures the integrity of data.
Objective	To prevent errors, loss, unauthorized modification or misuse of information in applications.
Framework Reference	**NIST CSF:** PR.IP-2 **NIST 800-53r5:** SA-3, SA-4, SA-8, SA-10, SA-11

3.11.2 Cryptographic Controls

Policy	Cryptographic controls shall be employed to protect information in accordance with the NRA Data Classification and Handling Policy.
Principle	Organizations should employ cryptographic controls to protect certain types of information that they consider to be highly sensitive in nature and for which other controls do not provide adequate protection.
Control:	To protect the confidentiality, authenticity, or integrity of information by cryptographic means.
Framework Reference	**NIST CSF:** PR.DS-1 **NIST 800-53r5:** MP-2, MP-3, MP-4, MP-5, MP-6, MP-7, MP-8, SC-28

3.11.3 Security of System Files

Policy	All IT projects and support functions shall be carried out in a secure manner. In particular, controls shall be implemented to ensure that the integrity of system files shall be maintained at all times.
Principle	Organizations must ensure that their IT projects and support activities are conducted in a secure manner.

Objective	To ensure the security of system files.
Framework Reference	**NIST CSF:** PR.DS-6 **NIST 800-53r5:** SI-7, SI-10

3.11.4 Separation of Development and Production Environments

Policy	Development and production environments shall be separated and shall adhere to the following: • Development teams shall be restricted from administrative level access to production systems. • Development and production software shall be maintained on different systems where possible. • Development and production software shall be maintained on a logically separated network where possible. • Compilers, editors and other system utilities shall not be accessible from operational systems when not required. • Production data should not be used in development environments wherever possible. Should production data be required in a development environment all restricted data should be masked, truncated, or otherwise obfuscated in a manner consistent with the NRA Data Obfuscation Standard.
Principle	Organizations must ensure that their IT projects and support activities are conducted in a secure manner.
Objective	To maintain the integrity and availability of information and information processing facilities.
Framework Reference	**NIST CSF:** PR.IP-4; PR.PT-5 **NIST 800-53r5:** CP-4, CP-6, CP-7, CP-8, CP-9, CP-11, CP-12, CP-13, PE-11, PL-8, SC-6

3.11.5 Development General Security Controls

Policy	All Association systems coding and development shall be carried out in a secure manner. The Association shall document Secure Development standards and DevSecOps practices for developers to adhere to (e.g., MITRE CWE, OWASP, etc…) In particular, the security of application system software and information shall be maintained at all times. • All developed software solutions shall include appropriate security, access and audit controls in accordance with the Association Logging and Monitoring Policy.

	• All software development shall follow standardized and documented procedures that include design, implementation, testing, hardening and modification. • All internally-developed software code shall be required to successfully pass Security approved code level testing and review prior to implementation. • Security requirements shall be identified and agreed upon prior to the development of any system or solution. • Security requirements shall be identified during the planning phase of any project, and shall be included as part of the overall business case. • To speed the development process and enhance the Association's security stance, where applicable, existing approved security architecture shall be included in new projects.
Principle	Organizations must ensure that their project and support environments are strictly controlled.
Objective	To maintain the security of application system software and information.
Framework Reference	**NIST CSF:** PR.IP-2 **NIST 800-53r5:** SA-3, SA-4, SA-8, SA-10, SA-11

3.11.6 Technical Vulnerability Management

Policy	A process shall be established to identify and counter technical vulnerabilities in the Association's information systems.
Principle	Organizations should be aware of the risks to their information and to their information systems that are due to technical vulnerabilities. Organizations should take the necessary steps to counter these risks by neutralizing or otherwise protecting against the effects of the technical vulnerabilities.
Objective	To reduce risks resulting from the exploitation of published technical vulnerabilities.
Framework Reference	**NIST CSF:** PR.IP-12; DE.CM-8 **NIST 800-53r5:** RA-1, RA-3, RA-5, SI-2

3.11.7 Web Services

Policy	Where web services are used in applications and systems their deployment shall be in accordance with industry and information security best practice.
Principle	Organizations should ensure that the use of web services does not compromise its information security status.
Objective	To ensure that the use of web services does not compromise the security of the Association's systems and data.

Framework Reference	**NIST CSF:** PR.IP-1; PR.IP-2 **NIST 800-53r5:** CM-1, CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-3, SA-4, SA-8, SA-10, SA-11

3.11.8 Mobile Applications

Policy	Mobile applications shall be developed in accordance with industry and information security best practice.
Principle	Organizations should ensure that the use of mobile applications does not compromise its information security status.
Objective	To ensure that the use of mobile applications does not compromise the security of the Association's systems and data.
Framework Reference	**NIST CSF:** PR.IP-2 **NIST 800-53r5:** SA-3, SA-4, SA-8, SA-10, SA-11

3.11.9 System Planning and Acceptance

Policy	To ensure the future availability of adequate systems capacity and resources, advanced systems planning, and preparation shall be conducted. Operational requirements for new systems shall be established, documented, and tested prior to their acceptance and use. Asset/System Owners shall be responsible for working with IT to monitor and plan for capacity limitations and bottlenecks. Asset/System Owners responsible for production and development environments shall develop and document acceptable standards for integration of new systems into areas of their responsibility. Where applicable these standards shall include: • Error recovery, restart procedures and contingency plans. • Agreed set of security controls. • Effective manual procedures. • Business continuity arrangements. • Evidence that integration of a new system will not adversely affect existing systems. • Evidence that consideration has been given to the effect of the new system on overall security of the environment.

	All systems being considered for use within a production or development environment shall be approved by the environment's Asset Owner as being acceptable prior to introduction or integration into said environment.
Principle	Organizations should ensure that their planning processes cover issues such as future systems capability. Projections of future capacity requirements should be made in order to reduce the risk of future systems overload.
Objective	To minimize the risk of systems failures.
Framework Reference	**NIST CSF:** PR.IP-2; PR.DS-4 **NIST 800-53r5:** SA-3, SA-4, SA-8, SA-10, SA-11, AU-4, CP-2, PE-11, SC-5

3.11.10 Capacity Planning

Policy	Asset owners shall be responsible for working with System Owners to monitor and plan for capacity limitations and bottlenecks.
Principle	Organizations should ensure that their planning processes cover issues such as future systems capability. Projections of future capacity requirements should be made in order to reduce the risk of future systems overload.
Objective	To minimize the risk of systems failures by ensuring systems have appropriate resources allocated.
Framework Reference	**NIST CSF:** PR.IP-2 **NIST 800-53r5:** SA-3, SA-4, SA-8, SA-10, SA-11

3.11.11 Application Programming Interface (API) Security

Policy	In all cases where the Association exposes its data and systems to third party applications by means of Application Programming Interfaces (APIs) for the purposes of connecting to the Association, integrating with the Association and extending the Association's business presence and capability, the APIs shall: • Be subject to formal governance • Be managed effectively • Be implemented securely • Enforce appropriate restrictive access controls, including authentication and authorization mechanisms
Principle	Organizations which expose their data and systems to third party applications should do so in a managed and secure manner by use of secure Application Programming Interfaces (APIs) that enforce appropriate restrictive access controls.

Objective	To ensure that all APIs enforce control access to data and systems.
Framework Reference	**NIST CSF:** PR.AC-4:5 **NIST 800-53r5:** AC-1, AC-2, AC-3, AC-4, AC-5, AC-6, AC-10, AC-14, AC-16, AC-24, SC-7, SC-10, SC-20

3.12 *Incident Management*

3.12.1 Reporting Information Security Events and Weaknesses

Policy	Appropriate processes shall be implemented to ensure that information security events, and weaknesses associated with the Association's information systems, are reported quickly through the appropriate management channels. Security incident response procedures shall be conducted and carried out as specified within NRA's Security Incident Response Plan.
Principle	Incidents affecting an organization's information security should be reported through appropriate management channels as quickly as possible.
Objective	To ensure that information security events and weaknesses associated with the Association's information systems are communicated in a manner allowing timely corrective action to be taken.
Framework Reference	**NIST CSF:** RS.CO-2:3 **NIST 800-53r5:** AU-6, IR-4, IR-6, IR-8, CP-2

3.12.2 Management of Information Security Incidents

Policy	Appropriate measures shall be implemented to ensure the effective management and orderly response to information security incidents.
Principle	Incidents affecting an organization's information security should be managed consistently and effectively. Any learning points should be noted for the overall improvement of the organization's information security position.
Objective	To ensure that a consistent and effective approach is applied to the management of information security incidents.

Framework Reference	**NIST CSF:** RS.RP-1; RS.CO-1:5; RS.AN-1:5; RS.MI-1:3; RS.IM-1:2 **NIST 800-53r5:** CP-2, CP-3, CP-10, IR-3, IR-4, IR-6, IR-8, AU-6, PE-6, SI-5, PM-15

3.13 *Business Continuity Management (BCM)*

3.13.1 Information Security Aspects of BCM

Policy	A business continuity management process shall be implemented to reduce the disruption caused by disasters and security failures (which may be the result of natural disasters, accidents, equipment failures and deliberate actions) to an acceptable level through a combination of preventative and recovery controls. Where required to be specifically documented, Information Security issues must be clearly identified. Apart from where specified, Information Security provision shall be assumed to comply with the policy.
Principle	Organizations should implement a range of measures to protect their business activities from the impact of disasters and other events that could seriously and adversely threaten the organization's continued existence.
Objective	To counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption.
Framework Reference	**NIST CSF:** RC.RP-1 **NIST 800-53r5:** CP-10, IR-4, IR-8

3.13.2 Information Security Aspects of DR and CM Planning

Policy	A Disaster Recovery (DR) and Crisis Management (CM) process shall be implemented to reduce the disruption caused by disasters and security failures (which may be the result of natural disasters, accidents, equipment failures and deliberate actions) to an acceptable level via recovery controls. Where required to be specifically documented, Information Security issues shall be clearly identified. Apart from where specified, Information Security provision shall be assumed to comply with the relevant Information Security Policy.
Principle	Organizations should implement a range of measures to protect their business activities from the impact of disasters that could seriously and adversely threaten the organization's continued existence.
Objective	To counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption.
Framework Reference	**NIST CSF:** RC.RP-1; RC.IM-1:2; RC.CO-1:3 **NIST 800-53r5:** CP-2, CP-10, IR-4, IR-8

3.13.3 Compliance with Legal Requirements

Policy	The Association shall conduct its business in accordance and compliance with all applicable laws, regulations, and statutes, and contracts
Principle	Organizations should conduct their business in accordance with all applicable laws, regulations and statues.
Objective	To avoid breaches of any law, statutory, regulatory or contractual obligations and of any security requirements.
Framework Reference	**NIST CSF:** ID.GV-3 **NIST 800-53r5:** PM-12, PM-16, RA-3, RA-10, SI-5

3.13.4 Compliance with Baseline Standards

Policy	The Association shall ensure that, as a minimum, its applications, systems, platforms and infrastructure items comply with the Association's Baseline Standards for asset protection.
Principle	Organizations should seek assurance that, as a minimum, their systems conform to an agreed set of standards which have established as a minimum set, or baseline.
Objective	To ensure that all the Association's applications, systems, platforms and infrastructure items comply with the Association's Baseline Standards.
Framework Reference	**NIST CSF:** PR.IP-1 **NIST 800-53r5:** CM-1, CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10

3.13.5 Compliance with Technical Standards

Policy	The Association shall ensure that its applications, systems, platforms and infrastructure items comply with the Association's technical standards.
Principle	Organizations should seek assurance that their systems conform to an agreed set of technical standards.
Objective	To ensure that all the Association's applications, systems, platforms and infrastructure items comply with the Association's Technical Standards.
Framework Reference	**NIST CSF:** PR.IP-1 **NIST 800-53r5:** CM-1, CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10

4 References

The following strategic documents, policies and standards may provide more detail in specific areas as they relate to this document.

- NRA Code of Conduct
- Risk Register
- Disaster Recovery and Crisis Management Plan
- Acceptable Use Policy
- Encryption and Key Management Standard
- External Supplier Security Standard
- Identity and Access Management Standard
- Information Classification and Handling Standard
- Logging and Monitoring Standard
- Mobile Computing and Remote Access Standard
- Network Infrastructure and Configuration Standard
- Network Segmentation and Zoning Standard
- Vulnerability & Patch Management Standard
- Physical Security Standard
- Secure Application Development Standard
- Secure Deletion and Disposal Standard
- Security Incident Management Standard

ADDENDUM FOR EDUCATIONAL INSTITUTIONS

1. General: Pursuant to the Contract ("**Contract**"), Vendor has agreed to sell to BOCES and BOCES has agreed to buy from Vendor certain products ("**Products**") and/or services ("**Services**") as set forth in such Contract. This Addendum for Educational Institutions ("**Vendor Addendum**") is hereby deemed to be attached to and made a part of the Contract and any reference to the Contract is intended to include this Vendor Addendum. If there is a conflict between this Vendor Addendum and any term in the Contract or any other document issued by District, this Vendor Addendum shall prevail. Instructors and other BOCES officials should review NRAS' Privacy Policy (at www.servsafe.com/Privacy-Policy) and Terms of Use (https://www.servsafe.com/Terms-of-Use).

2. Student or Parent/Guardian Consent: Because Vendor will not have any direct contact or correspondence with any of the students of BOCES, BOCES hereby agrees to obtain all necessary prior written consents ("**Consent**") from each student using the Products or Services (or such student's parent/guardian if the student is a minor) for Vendor to use and disclose such student's personally identifiable information, including "educational records" as defined by the Family Educational Rights and Privacy Act ("**FERPA**"), 20 U.S.C. § 1232(g), as reasonably necessary for the provision of the Products or Services. Such Consent to be obtained by BOCES, which shall be in substantially the form provided herewith, shall authorize and include all permissions and consents of each student or parent/guardian (as applicable) required by FERPA and any other applicable local, state or federal statute or regulation for Vendor to:

   a. share or publicly disclose the student's certification status, educational training, test scores and such other personally identifiable information as reasonably required to attest to the certification status or other relevant information for users of the Products or Services;

   b. share with prospective employers or current employers of the student the certification status and professional training of such student; and

   c. provide information regarding additional Products or Services that Vendor believes may advance or enhance the workforce development or career opportunities of students.

3. Acknowledgement; Indemnification: BOCES acknowledges and agrees that Vendor's Products or Services include the public posting or disclosure of training and certification undertaken by students in order to advance work and career opportunities. BOCES shall provide Vendor with a copy of a student's Consent upon the reasonable request of Vendor or any applicable legal authority. BOCES acknowledges that Vendor is relying upon the performance of BOCES under this Addendum for compliance, and it shall indemnify and hold Vendor harmless from any claims related to the failure of BOCES and/or its applicable schools or educational institutions in obtaining such required permission or Consent.

This Vendor Addendum has been accepted and agreed with respect to the Contract, as evidenced by a signature of an authorized representative of each party below:

NATIONAL RESTAURANT ASSOCIATION SOLUTIONS, LLC	**JEFFERSON-LEWIS BOCES**
By: Alisha Gulden	By:
Name: Alisha Gulden	Name:
Title: Sr Vice President of Sales	Title:
Date: 06/17/2024	Date:

STUDENT PARTICIPATION FORM

The undersigned student attending the school designated below (the "Educational Institution") seeks to use certain training and certification programs (the "Programs") offered by National Restaurant Association Solutions, LLC ("NRAS"). In connection with the student's use of the Programs and related services, the student may provide NRAS with the student's personally identifiable information ("PII"), including name, address, date of birth and possibly social security number, for purposes of reporting academic or certification results to the Educational Institution or potential employers, etc. NRAS will use this information in compliance with its Privacy Policy (at www.servsafe.com/Privacy-Policy) to:

1. Administer the Programs in cooperation with the Educational Institution;
2. Share with the Educational Institution, prospective employers or current employers of a student the exam results, certification status and professional training of such student;
3. Post accreditation, certification or training results to its public website for access by employers, educators or others;
4. Share or publicly disclose such other education records or PII as reasonably required to attest to a student's certification status or for other purposes relevant to participants in the Programs; and
5. Provide information regarding additional training and certification programs that may advance or enhance the student's workforce development or career opportunities.

Pursuant to the Family Educational Rights and Privacy Act, 20 U.S.C. § 1232(g) ("FERPA") and any other applicable federal, state and local laws and regulations (collectively, "Privacy Laws"), consent by parents/guardians of students who are minors or adult students may be required for the student's education records or PII to be disclosed and used as set forth above. For additional information regarding your student privacy rights and use of such information, please review the Privacy Laws and NRAS' Privacy Policy (at www.servsafe.com/Privacy-Policy). Students should review the Privacy Policy and NRAS's Terms of Use (https://www.servsafe.com/Terms-of-Use) prior to accessing the Program.

This Student Participant Consent Form permits a parent, guardian or adult student to authorize the release and use of the student's education records and PII as provided herein. Information cannot be released and the student may not use the Programs or related services until a completed form is returned to the Educational Institution.

By signing below, you consent to the disclosure and use of the below-named student's education records and PII as set forth herein, and acknowledge that (1) you have the right not to consent, (2) you have a right to inspect the student's education records, and (3) you have the right to revoke this consent by provided express written notice at any time and this consent will remain in effect until such revocation is received.

Student's Full Name:	
Student Identifier (if any):	
Name of Educational Institution:	
Signature of Adult Student or Authorized Parent/Guardian (if student is under 18):	
Printed Name of Signatory:	
Date:	