

**Supplemental Agreement between the
Hewlett-Woodmere Union Free School District**

And

Seneca Consulting Group

Supplemental Agreement dated this 1st day of July, 2023 between the Hewlett-Woodmere Union Free School District (the "District"), located at One Johnson Place, Woodmere, NY 11598, and Seneca Consulting Group (the "Contractor") located at 960 Wheeler Road, #5367, Hauppauge, NY 11788.

WHEREAS, the District and Contractor have entered into a contract or other written agreement (hereinafter the "Agreement") whereby the Contractor may receive Student Data or Teacher or Principal Data, as those terms are defined in Education Law §2-d and 8 NYCRR 121.1; and

WHEREAS, the District and Contractor wish to enter into an agreement in order to comply with Education Law §2-d and 8 NYCRR Part 121 (hereinafter "Supplemental Agreement").

NOW THEREFORE, in consideration of the mutual promises below, the District and Contractor agree as follows:

1. Defined Terms: Unless otherwise indicated below or elsewhere in this Supplemental Agreement, all capitalized terms shall have the meanings provided in Education Law §2-d and Section 121.1 of the Regulations of the Commissioner of Education (hereinafter "Regulations").

a. "Educational Agency" shall generally have the same meaning as the term Educational Agency at Education Law §2-d(1)(c) and Section 121.1(f), and in reference to the party to this Agreement shall mean the Hewlett-Woodmere Union Free School District.

b. "Third Party Contractor" shall mean any person or entity, other than an Educational Agency, that receives Student Data or Teacher or Principal Data from an Educational Agency pursuant to a contract or other written agreement for purposes of providing services to such Educational Agency, including but not limited to data management or storage services, conducting studies for or on behalf of such Educational Agency, or audit or evaluation of publicly funded programs. With reference to this agreement, "Third Party Contractor" shall be synonymous with "Contractor" and shall also include any and all subcontractors, persons or entities with whom the Contractor shares Student Data and/or Principal or Teacher Data pursuant to a contract or other written agreement for purposes of providing services to such Educational Agency, including but not limited to data management or storage services, conducting studies for or on behalf of such Educational Agency, or audit or evaluation of publicly funded programs.

c. "Student" means any person attending or seeking to enroll in an Educational Agency.

d. "Student Data" means Personally Identifiable Information of a "Student."

e. "Eligible Student" means a Student who is eighteen years or older.

f. "Parent" means a parent, legal guardian, or personal in parental relation to a Student.

g. "Building Principal" or "Principal" means a building principal subject to annual performance evaluation review under Education Law §3012-c.

h. "Classroom Teacher" or "Teacher" means a teacher subject to annual performance evaluation review under Education Law §3012-c.

i. "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.

j. "Personally Identifiable Information" shall have the following meanings:

i. As applied to Student Data, shall mean Personally Identifiable Information as defined in 34 CFR 99.3 implementing the Family Educational Rights and Privacy Act (FERPA)

ii. As applied to Teacher or Principal Data, shall mean Personally Identifiable Information as that term is defined in Education Law §3012-c.

2. The District has developed the Parents Bill of Rights for Data Privacy and Security, the terms of which are applicable to the Agreement between the District and Contractor and are incorporated into this Supplemental Agreement. The Parents Bill of Rights for Data Privacy and Security states:

Pursuant to New York State Education Law §2-d, parents, legal guardians and persons in parental relation to a student are entitled to certain rights with regard to their child's personally identifiable information, as defined by Education Law §2-d. The Hewlett-Woodmere Public School District, in recognition of the risk of identity theft and unwarranted invasion of privacy, affirms its commitment to safeguarding student personally identifiable information (PII) in educational records from unauthorized access or disclosure in accordance with State and Federal law. This document contains a plain-English summary of such rights.

1. Student PII will be collected and disclosed only as necessary to achieve educational purposes in accordance with State and Federal Law.

2. A student's personally identifiable information cannot be sold or released for any commercial or marketing purposes by the District or any a third party contractor. The district will not sell student personally identifiable information and will not release it for marketing or commercial purposes, other than directory information released by the district in accordance with district policy;
3. Parents have the right to inspect and review the complete contents of their child's educational records maintained by the Hewlett-Woodmere Public Schools. (for more information about how to exercise this right, see 5500-R);
4. State and Federal Laws, such as NYS Education Law §2-d and the Family Educational Rights and Privacy Act, protect the confidentiality of students' personally identifiable student information. Safeguards associated with industry standards and best practices, including, but not limited to, encryption, firewalls, and password protection must be in place when data is stored or transferred;
5. A complete list of all student data elements collected by New York State is available for review at the following website:

a. <http://www.p12.nysed.gov/irs/sirs/documentation/NYSEDstudentData.xlsx>

6. The list may also be made available by writing to:

Chief Privacy Officer
New York State Education Department
89 Washington Avenue
Albany, NY 12234

7. Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed to:

Hewlett-Woodmere Public Schools
1 Johnson Place
Woodmere, New York 11598
(516) 792-4802

OR

Complaints can also be directed to the New York State Education Department online at <http://nysed.gov.data-privacy-security>, by mail to the

Chief Privacy Officer
New York State Education Department
89 Washington Avenue
Albany, NY 12234

Email: privacy@mail.nysed.gov

Telephone at 518-474-0937

8. Parents have the right to be notified in accordance to applicable laws and regulations if a breach or unauthorized release of their student's PII occurs.
9. Parents can expect that educational agency workers who handle PII will receive annual training on applicable federal and state laws, regulations, educational agency's policies and safeguards which will be in alignment with industry standards and best practices to protect PII.
10. In the event that the District engages a third-party provider to deliver student educational services, the contractor or subcontractor will be obligated to adhere to State and Federal Laws to safeguard student PII. Parents can request information about third party contractors by contacting

Amanda Kavanagh
Data Protection Officer
Hewlett-Woodmere Public Schools
1 Johnson Place
Woodmere, New York 11598
(516) 792-4892
akavanagh@hewlett-woodmere.net

or can access the information on the District's website:
<https://www.hewlett-woodmere.net/Page/11125>

Each contract with a third-party contractor which will receive student data, or teacher or principal data will include information addressing the following:

- a. The exclusive purposes for which the student data or teacher or principal data will be used.
- b. How the third-party contractor will ensure that the subcontractors, persons or entities that the third-party contractor will share the student data or teacher or principal data with, if any, will abide by data protection and security requirements.
- c. When the agreement expires and what happens to the student data or teacher and principal data upon expiration of the agreement.
- d. If and how a parent, student, a student over eighteen years of age, teacher or principal may challenge the accuracy of the student data or teacher or principal data that is collected; and
- e. Where the student data or teacher or principal data will be stored, and the security protections taken to ensure such data will be protected, including whether such data will be encrypted.

7. Third-party contractors are also required to:

- a. Provide training on federal and state law governing confidentiality to any officers, employees, or assignees who have access to student data or teacher or principal data;
- b. Limit internal access to education records to those individuals who have a legitimate educational interest in such records.
- c. Not use educational records for any other purpose than those explicitly authorized in the contract;
- d. Not disclose personally identifiable information to any other party (i) without the prior written consent of the parent or eligible student; or (ii) unless required by statute or court order and the third-party contractor provides a notice of the disclosure to the New York State Education Department, board of education, or institution that provided the information no later than the time the information is disclosed, unless providing notice of the disclosure is expressly prohibited by the statute or court order;
- e. Maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of personally identifiable student information in its custody;
- f. Use encryption technology to protect data while in motion or in its custody from unauthorized disclosure as specified in Education Law §2-d;
- g. Notify the Hewlett-Woodmere Public Schools of any breach of security resulting in an unauthorized release of student data or teacher or principal data, in the most expedient way possible and without unreasonable delay;
- h. Provide a data security and privacy plan outlining how all state, federal and local data security and privacy contract requirements will be implemented over the life of the contract;
- i. Provide a signed copy of this Bill of Rights to the Hewlett-Woodmere Public Schools thereby acknowledging that they are aware of and agree to abide by this Bill of Rights.

8. This Bill of Rights is subject to change based on regulations of the Commissioner of Education and the New York State Education Department's Chief Privacy Officer, as well as emerging guidance documents.

3. As required by Education Law §2-d(3)(c) and Section 121.3 of the Regulations, the Contractor shall comply with the Data Security and Privacy Plan which is attached to this Agreement.

4. As required by Education Law §2-d(5)(e), the Contractor hereby agrees that any officers or employees of the Contractor, including any subcontractors or assignees, who have access to Student Data or Teacher or Principal Data will have or will receive training on the Federal and

New York State laws governing confidentiality of Student Data and/or Principal or Teacher Data prior to receiving access.

5. As required by Education Law §2-d(5)(f), the Contractor hereby agrees that it shall:
 - a. Limit internal access to education records to those individuals that are determined to have legitimate educational interests;
 - b. Not use the educational records for any other purposes than those explicitly authorized in the Agreement or this Supplemental Agreement;
 - c. Except for authorized representatives of the Contractor to the extent they are carrying out the Agreement or this Supplemental Agreement, not disclose any Personally Identifiable Information to any other party:
 - i. Without the prior written consent of the Parent or Eligible Student; or
 - ii. Unless required by statute or court order and the party provides a notice of the disclosure to the State Education Department, District Board of Education, or institution that provided the information no later than the time the information is disclosed, unless providing notice of the disclosure is expressly prohibited by the statute or court order.
 - d. maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of personally identifiable student information in its custody;
6. Breach and unauthorized release of Personally Identifiable Information:
 - a. In accordance with Education Law §2-d(6) and Section 121.11 of the Regulations, the Contractor shall be required to notify the District of any breach of security resulting in an unauthorized release of Student Data and/or Principal or Teacher Data by the Contractor or its subcontractors or assignees in violation of applicable state or federal law, the Parents Bill of Rights for Student Data Privacy and Security, the data privacy and security policies of the District and/or binding contractual obligations relating to data privacy and security, in the most expedient way possible and without unreasonable delay. The District shall, upon notification by the Contractor, be required to report to the Chief Privacy Officer, who is appointed by the State Education Department, any such breach of security and unauthorized release of such data.
 - b. In the case of an unauthorized release of Student Data, the District shall notify the Parent or Eligible Student of the unauthorized release of Student Data that includes Personally Identifiable Information from the student records of such Student in the most expedient way possible and without unreasonable delay. In the case of an unauthorized

release of Teacher or Principal Data, the District shall notify each affected Teacher or Principal of the unauthorized release of data that includes Personally Identifiable Information from the Teacher or Principal's annual professional performance review in the most expedient way possible and without unreasonable delay.

c. In the case of notification to a Parent, Eligible Student, Teacher or Principal due to the unauthorized release of student data by the Contractor, or its subcontractors or assignees, the Contractor shall promptly reimburse the educational agency for the full cost of such notification, as required by Education Law §2-d(6)(c).

7. Miscellaneous:

a. The District and Contractor agree that if applicable laws change and/or if the Commissioner of Education implements Regulations which affects the obligations of the parties herein, this Agreement shall be deemed to incorporate such changes as necessary in order for the District and the Contractor to operate in compliance with the amendment or modified requirements under the applicable laws or regulations.

b. Any ambiguity in this Agreement shall be resolved in favor of a meaning that permits the District to comply with the applicable laws or regulations.

c. Nothing express or implied in this Agreement is intended to confer upon any person other than the District, Contractor and their respective successors and assigns any rights, remedies, obligations or liabilities.

IN WITNESS WHEREOF, the Parties hereto have duly executed this Agreement.

Seneca Park Consulting Group, LLC

By: [Signature]

Print Name: Daniel C. Opanante

Title: President

Date: 8/7/2023

**HEWLETT-WOODMERE UNION
FREE SCHOOL DISTRICT**

By: [Signature]

Print Name: Marie Donnelly

Title: Assistant Superintendent
for Finance and Personnel

Date: 8/29/2023

Data Security and Privacy Plan (DSPP)

Prepared by:
Seneca Risk Consulting Group, LLC
2022

I. Objective and Scope

In providing Affordable Care Act Consulting, Seneca Risk Consulting Group acknowledges that we have a serious obligation to help our clients protect the confidentiality data that we receive. As an Affordable Care Act Consultant for your District, we recognize that we share certain responsibilities to protect the security and privacy of sensitive data that is collected by the district and processed by our systems. This Data Security and Privacy Plan (DSPP) outlines the administrative, technical, and physical safeguards used to meet these responsibilities.

Educational data housed in Seneca Risk Consulting Group systems, including attendance payroll and personal information protected by the Family Education Rights and Privacy Act (FERPA). Personally identifiable information (PII) of staff is protected under FERPA, PPRA, COPPA and other federal, state and local regulations, including NY State Education Law section 2-d. Seneca Risk Consulting Group's Privacy Policy strictly prohibits the sale of sensitive staff data under any circumstances, or the unauthorized sharing of that data with other parties. Data collected is only used for the approved purposes specified in agreements between Seneca Risk Consulting Group and the client.

II. Data Security and Privacy Obligations

A. Relationship Between Security and Privacy

Significant overlap exists between the concepts of data security and data privacy; thus our approach to compliance has always been aimed at providing both, through multiple layers of controls designed to support our clients' policies.

B. Shared Responsibility

Privacy regulations define several distinct roles with respect to data:

Data subject/owner	the individual who is described or identified	Staff
Data controller	organization collecting the data for some defined purpose	client school or district

Data processor	provider of technology/services in support of the defined purpose	Seneca Risk Consulting Group
----------------	---	------------------------------

Note that data privacy protection requires cooperation between the data controller (District) and the data processor (Seneca Risk Consulting Group). In most cases, there is no direct relationship between Seneca Risk Consulting Group and the data subject/owner. The District, as data controller, has the primary responsibility for ensuring that data is protected appropriately throughout all phases of its life cycle.

The District's role is to:

- define their business needs or purpose for collecting data.
- Designate personnel responsible for data privacy matters
- Establish privacy policies and practices aligned with the defined purpose
- communicate directly with students/staff/parents regarding data collection and use
- obtain consent for data collection as appropriate.
- define the conditions under which the data is no longer needed and should be purged (data retention/disposal policy)
- provide awareness training to ensure that their staff, administrators, and volunteers know how to handle sensitive data properly.

Seneca Risk Consulting Group 's role is to:

- Communicate privacy objectives to internal users and clients
- provide the technical means to process data securely.
- protect data while it is in our custody.
- securely remove it when it is no longer needed
- provide awareness training to ensure that our employees know how to handle sensitive data properly

Note that in most cases Seneca Risk Consulting Group does not interact directly with the data subjects; therefore it is the responsibility of the District to obtain explicit consent where appropriate. Under the FERPA "school official exception", explicit consent is not needed when data is collected for the purpose of providing the agreed-upon services, since Seneca Risk Consulting Group is acting as an agent of the District.

C. Defining the Purpose

Seneca Risk Consulting Group's Affordable Care Act Agreement limits the "purpose" of its systems to the provision of supporting the client with compliance under the Affordable Care Act, specific to the employer Shared Savings requirements under §4980H(a)(b) and the IRS Reporting Requirements under §6055 and §6056:

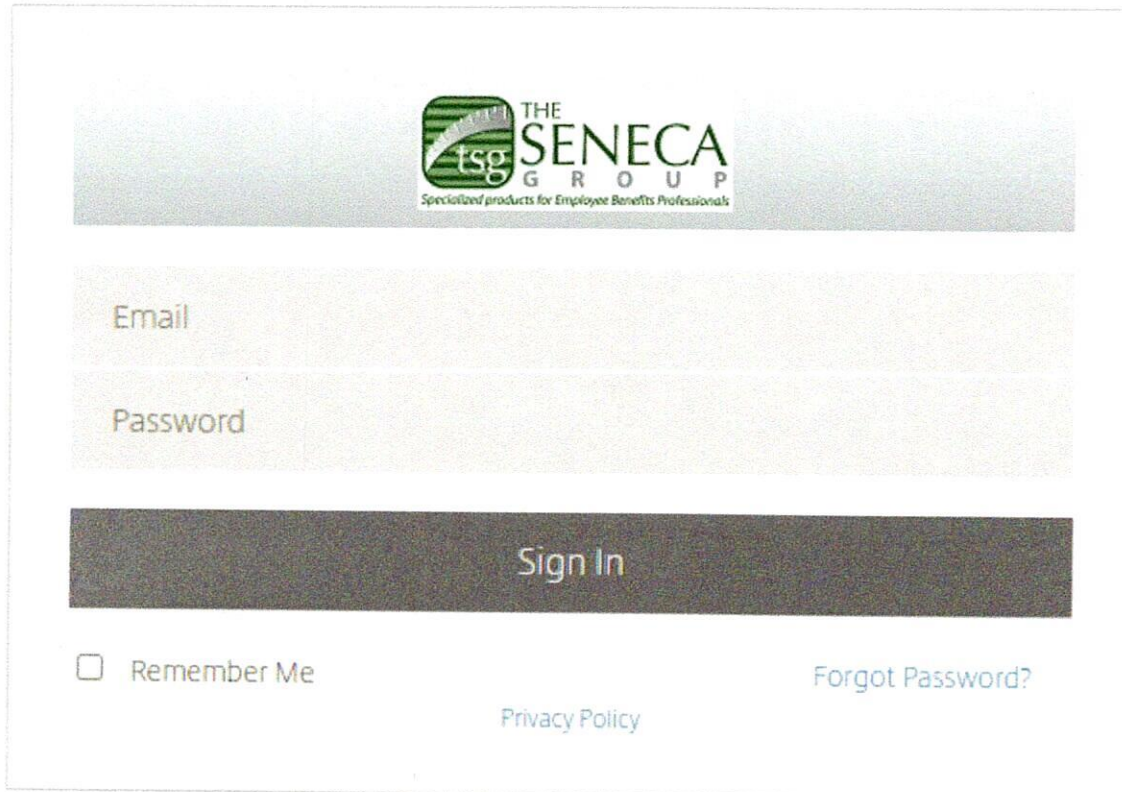
- §4980H (a) Requires "Applicable Large Employers" (Employers with at least 50 "full-time employees" to offer Minimum essential health insurance coverage to at least 95% of its "full-time employees"
- §4980H (b) Requires "Applicable Large Employers" (Employers with at least 50 "full-time employees" to offer "Affordable" Minimum essential health insurance coverage to all its "full-time employees"
- §6055- Applicable Large Employers who provide a self-insured health plan must report to the IRS all enrollees in that plan (including dependents) and each calendar month that they were enrolled in that self-insured plan. This requirement is met through either the IRS Form 1095C Section III, or IRS Form 1095B Part IV.
- §6056- Requirement to report to the IRS whether they offered their Full-time employees and their employees dependents the opportunity to enroll in "Minimum Essential Coverage", and to include if an offer was made, and if the offer was considered affordable. This requirement is met through the IRS Form 1095C Part II.

D. Allowed and Prohibited Access/Use/Disclosure

Staff data (Student data is not provided to Seneca), whether provided to Seneca Risk Consulting Group by the District or generated by Seneca Risk Consulting Group through normal system operation, is only to be used for the above defined purposes. Within Seneca Risk Consulting Group, data is only to be shared with Approved District contracts who can access it in connection with the agreed-upon services. All employees, whether they have access, receive security and privacy awareness training.

To provide the agreed-upon services, Seneca Risk Consulting Group must initially receive data from the District's Payroll system and Self-Funded Health plan or both and also pass some data back. Data Integration standards and processes are in place to ensure that data is transferred securely between the two entities. The following Process has been established:

Clients upload all protected information through Seneca Risk Consulting Group's Secure web portal Citrix Share file. With ShareFile, you have a platform that provides industry-leading security standards when sharing confidential files. Files are kept secure during transfer with SSL/TLS encryption protocols. In the cloud, storage of files is kept safe using AES 256-bit encryption



THE SENECA GROUP
Specialized products for Employee Benefits Professionals

Email

Password

Sign In

☐ Remember Me

[Forgot Password?](#)

[Privacy Policy](#)

Each Sharefile user, both Seneca Risk Consulting Group and Client, will receive a unique username and password to access the secure portal.

Seneca Risk Consulting Group staff will only share information with district, and the report to the IRS, to the extent necessary to provide the services described in the contract.

Seneca Risk Consulting Group will not disclose any personally identifiable information to any other party without prior written consent of the District, unless required by statute or court order. In this case we will provide a notice of such disclosure to the District no later than the time the information is disclosed, unless providing notice of the disclosure is expressly prohibited by statute or court order. Staff members are instructed on this through the yearly FERPA training. Any violation is met with strict disciplinary penalties, as outlined in our information security and privacy policies.

New staff orientation includes instructions on using Sharefile when sending or receiving staff data.

E. State/Local Data Privacy Regulations

In accordance with NY State Education Law section 2-d, each district must publish a Parents' Bill of Rights (PBOR), which outlines the District's specific student data privacy responsibilities and expectations.

Seneca Risk Consulting Group is also in compliance with federal privacy laws including HIPPA

training for Seneca Risk Consulting Group employees, adequate data protection measures, data

breach notification procedures, etc.

Other state and federal regulations outline similar requirements. Seneca Risk Consulting Group stays continuously updated on evolving privacy regulations and will work with your district to ensure that our clients compliance.

This section outlines the District's specific staff data privacy responsibilities (as a data controller) and defines Seneca Risk Consulting Group's role (as a data processor) in meeting each of them.

F. Standard Staff Data Privacy Practices

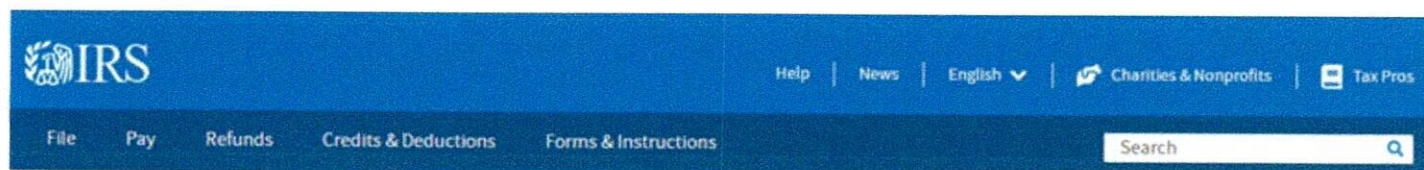
1. Restrictions on Use and Release of Information

Staff data (Seneca does not receive Student and visitor data), whether provided to Seneca Risk Consulting Group by the District or generated by Seneca Risk Consulting Group through normal system operation, is only to be used for the purposes defined in the Affordable Care Act Agreement.

In accordance with applicable data privacy laws and Seneca Risk Consulting Group's privacy policy, Seneca Risk Consulting Group will not sell a any personally identifiable information or release it for any commercial purposes.

Within Seneca Risk Consulting Group, access to staff data (Seneca does not receive student or community data) is only granted to individuals who need such access to perform their job functions in connection with the specific services outlined in the service agreement. Seneca Risk Consulting Group employees are prohibited from accessing this data for any other purpose and are made aware of this restriction through policy and training.

In order to provide the agreed-upon services, it may be necessary to share staff information with the Internal Revenue Service (IRS). Seneca Risk Consulting Group is an approved electronic filer with the IRS and submits the data required by the IRS through the IRS Secure Affordable Care Act Information System (AIS)



[Home](#) / [Tax Pros](#) / Affordable Care Act Information Returns (AIR)

Affordable Care Act Information Returns (AIR)

Enrolled Agents

Annual Filing Season Program Participants

Enrolled Retirement Plan Agents

Certified Professional Employer Organization (CPEO)

Enrolled Actuaries

E-File Providers

Modernized e-File

Online AIR Systems

[User Interface \(UI\) ACA Assurance Testing System \(AATS\)](#)

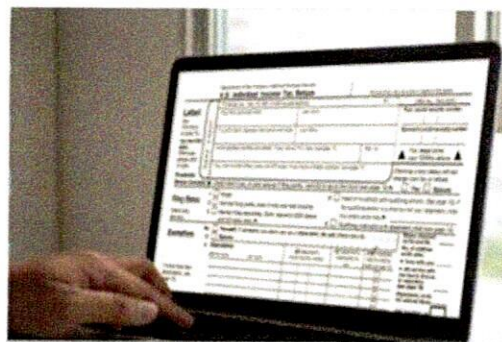
Log in to upload your test forms or scenarios.

[User Interface \(UI\) Production System](#)

Log in to upload your 1094 and 1095 forms.

[Automated Enrollment \(AE\) for ACA Providers](#)

Upload your certificates when transmitting through the Application to Application (A2A) channel. See [Publication 5308, Automated Enrollment for ACA Providers the Externals Guide](#) [PDF](#) for all activities.



AIR System Operational Status

[Check Status](#)

2. Right to Review

Seneca Risk Consulting Group acknowledges that staff have the right to inspect and review the complete contents of information submitted to the IRS. It is the District's responsibility to provide staff with access to this upon request.

Copies of all IRS data submitted by Seneca Consulting on the District's behalf is stored on Citrix Sharefile, and the District has access to it any anytime. Seneca would be happy to provide support to the District when accessing this information.

3. Reasonable Safeguards to Protect Confidentiality

Seneca Risk Consulting Group acknowledges that we have a responsibility to protect the confidentiality of personally identifiable information in our custody, throughout its entire lifecycle, using reasonable administrative, technical and physical safeguards associated with industry standards and best practices. Specific protection measures in use are described in Section III of this document.

4. Addressing Privacy Concerns and Complaints

Seneca Risk Consulting Group acknowledges that staff have the right to have complaints about possible breaches of data addressed. Complaints should be first directed to the appropriate School District personnel as defined in their policies and the District's published PBOR.

Seneca Risk Consulting Group is responsible for addressing data protection issues and concerns. Clients may contact Dan@senecaconsulting.com with any concerns about our privacy practices and data protection.

III. Protection of Personally Identifiable Information

A. Seneca Risk Consulting Group Security Strategy - Data Protection by Design and by Default

Seneca Risk Consulting Group systems are fully compliant with several comprehensive industry-recognized security standards. Significant overlap exists between the concepts of data security and data privacy; thus our approach to compliance has always been aimed at providing both, through multiple layers of controls designed to support our clients' defined policies.

We ensure data security using a combination of Preventive, Detective, and Organizational controls, including network architecture and configuration, software design, policies, procedures and other critical protective measures.

B. Organizational Controls

•
•

1. Roles and Responsibilities

Information security/privacy responsibilities at Seneca Risk Consulting Group are shared across multiple departments. Every effort is made to integrate security controls and processes into regular workflows and make them part of “business as usual”, to maintain a continuous state of compliance with applicable regulations.

2. Policies and Procedures

We maintain a full set of security policies covering the 3 major areas of security - confidentiality, integrity and availability. Specific topics include information sensitivity/classification, privacy obligations, system configuration standards, data retention, encryption, access control, software development guidelines, security monitoring and testing, awareness and training, employee screening, incident response and business continuity.

Policies are distributed to new employees as part of onboarding, reviewed throughout the year as part of ongoing risk assessment and updated according to business/technology changes when appropriate. Updated versions are published at least annually and distributed to employees for acknowledgement.

C. Infrastructure

Data protection starts with a secure infrastructure. All critical system components are housed in Seneca Risk Consulting Group 's secure data centers, which provide assurance of physical and environmental security.

- ♦ Primary – Hauppauge
- ♦ Secondary – Web and physical
back up

Physical access to these data centers is limited to a very small number of Seneca Risk Consulting Group employees.

Major components are Windows servers, primarily 2008 and 2012, which are each configured for a specific function (web server, database server, monitoring tools, etc) Servers are hardened using configuration standards based on CIS benchmarks and PCI-DSS requirements

The Seneca Risk Consulting Group network is segmented to isolate highly sensitive data . Firewall rules are defined to explicitly allow specific types of traffic based on documented business and deny the rest by default. Rules are reviewed regularly by SENECA and technical team to ensure that only the necessary traffic is being allowed. Intrusion detection and load balancing functions are integrated into the firewall Data in transit on our network is protected by TLS protocol.

D. Data Storage and Protection

Sensitive data that requires special handling falls into several categories:

- PII of Staff - name, address, Social Security Number / Tax Identification Number - subject to various privacy regulations, including
 - NY State Education Law Section 2-d
 - PPRA
 - COPPA

Staff data (Seneca does not receive Student data) will be securely stored in the following ways:

The table below lists data storage and protection methods for all classes of information stored and processed by all Seneca Risk Consulting Group products and services. Not all data classes pertain to all clients. For questions relating to data storage in your specific implementation, contact your Seneca Risk Consulting Group data integration specialist.

Storage location/medium	Data Class	Protective Controls
SQL databases	Staff PII	<ul style="list-style-type: none"> Physical security (data center) Logical access control (VPN with 2-factor authentication, Windows server login credentials, Oracle database login credentials) <p>Data structure - data is stored in a normalized manner which minimizes the repetition of personal information. Student and staff records are assigned sequential ID numbers, and are only referenced by those ID's in other tables. This means that no Personally Identifiable Information is directly attached to educational or financial information.</p>
Citrix Sharefile	Staff PII	<p>Physical security</p> <p>Logical access control (VPN with 2-factor authentication, Windows server login credentials, SFTP login credentials)</p>

E. System monitoring and testing

Seneca Risk Consulting Group continuously monitors its systems for unauthorized activity that may result in the exposure of sensitive data.

Daily log reviews are the responsibility of Seneca Staff. The purpose of the daily log monitoring process is to document unusual occurrences in order to spot potential system security and operational problems, including both internal and external threats. Logs are aggregated using centralized audit logging mechanisms (syslog, EventTracker) to allow for some automation of the review process, as well as correlation of events from different sources. Critical issues are picked up by semaphore alerts on a real-time basis.

- Cloud application usage and data sharing - we use a cloud access/SaaS monitoring solution to detect and remediate instances of employees sharing sensitive information in unauthorized ways (either deliberately or inadvertently)

Vulnerability scanning and penetration testing are also performed regularly. Results are reviewed by SENECA and technical teams and any issues are remediated in a timely manner to reduce the potential for exploit of system vulnerabilities from the outside.

IV. Breach notification requirements

Should Seneca Risk Consulting Group become aware of any unauthorized release of student data, in violation of applicable privacy laws, the parents' bill of rights, and/or binding contractual obligations relating to data privacy and security, we will notify the Organization's designated privacy official in the most expedient way possible and without unreasonable delay.

If there is valid reason to suspect a breach (i.e., clients report fraudulent activity on their accounts, or we see signs that someone has gained unauthorized remote or physical access to the data center), Seneca Risk Consulting Group incident response team will:

- check for common indicators of compromise to determine whether a breach has actually occurred. Notify
- CTO, SENECA, and application owners of findings.
- Conduct additional research as necessary to determine the extent of impact.

If it is determined that a breach has occurred, system(s) or system component(s) may need to be taken offline until they can be locked down with additional security measures (change passwords and certificates, update firewall settings, etc.) An official statement will be issued to clients, summarizing our findings and providing an estimated time frame for service restoration.

V. Data Retention and Disposal

Staff data (Seneca does not receive student data) will only be stored as long as the District legitimately needs it. Seneca Risk Consulting Group's data architecture makes it straightforward to remove an individual's data at the request of the data controller (client) if it is no longer needed for a legitimate business purpose.

What happens to the staff data upon contract termination or expiration?

Unless otherwise agreed-upon by the Parties in writing, Seneca Risk Consulting Group shall remove or overwrite all Data from Seneca Risk Consulting Group's systems following the effective date of termination or cancellation, in accordance with Seneca Risk Consulting Group's standard procedures.