EXHIBIT D

DATA SHARING AND CONFIDENTIALITY AGREEMENT

INCLUDING
PARENTS BILL OF RIGHTS FOR DATA SECURITY AND PRIVACY
AND
SUPPLEMENTAL INFORMATION ABOUT THE MLSA

1. Purpose

(a) This Exhibit supplements the Master License and Service Agreement ("MLSA") to which it is attached, to ensure that the MLSA conforms to the requirements of New York State Education Law Section 2-d and any implementing Regulations of the Commissioner of Education (collectively referred to as "Section 2-d"). This Exhibit consists of the terms of this Data Sharing and Confidentiality Agreement, a copy of Erie 1 BOCES' Parents Bill of Rights for Data Security and Privacy signed by the Vendor, and the Supplemental Information about the MLSA that is required to be posted on Erie 1 BOCES' website.

(b) To the extent that any terms contained within the MLSA, or any terms contained within any other Exhibits attached to and made a part of the MLSA, conflict with the terms of this Exhibit, the terms of this Exhibit will apply and be given effect. In the event that Vendor has online or written Terms of Service ("TOS") that would otherwise be applicable to its customers or users of its Product that is the subject of the MLSA, to the extent that any term of the TOS conflicts with the terms of this Exhibit, the terms of this Exhibit will apply and be given effect.

2. Definitions

Any capitalized term used within this Exhibit that is also found in the MLSA will have the same definition as contained within the MLSA.

In addition, as used in this Exhibit:

(a) "Student Data" means personally identifiable information, as defined in Section 2-d, from student records that Vendor receives from a Participating Educational Agency pursuant to the MLSA.

(b) "Teacher or Principal Data" means personally identifiable information relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of New York Education Law Sections 3012-c or 3012-d, that Vendor receives from a Participating Educational Agency pursuant to the MLSA.

(c) "Protected Data" means Student Data and/or Teacher or Principal Data to the extent applicable to Vendor's Product.

(d) "Participating Educational Agency" means a school district within New York State that purchases certain shared instructional technology services and software through a Cooperative Educational Services Agreement with a BOCES, and as a result is licensed to use Vendor's Product pursuant to the terms of the MLSA. For purposes of this Exhibit, the term also includes Erie 1 BOCES or another BOCES that is licensed to use Vendor's Product pursuant to the MLSA to support its own educational programs or operations.

3. **Confidentiality of Protected Data**

(a) Vendor acknowledges that the Protected Data it receives pursuant to the MLSA may originate from several Participating Educational Agencies located across New York State, and that this Protected Data belongs to and is owned by the Participating Educational Agency from which it originates.

(b) Vendor will maintain the confidentiality of the Protected Data it receives in accordance with federal and state law (including but not limited to Section 2-d) and Erie 1 BOCES's policy on data security and privacy. Vendor acknowledges that Erie 1 BOCES is obligated under Section 2-d to adopt a policy on data security and privacy. Erie 1 BOCES will provide Vendor with a copy of its policy. Vendor and Erie 1 BOCES agree to engage in good faith negotiations to modify this Data Sharing Agreement to the extent necessary to ensure Vendor's continued compliance with Section 2-d.

4. **Data Security and Privacy Plan**

Vendor agrees that it will protect the confidentiality, privacy and security of the Protected Data received from Participating Educational Agencies in accordance with Erie 1 BOCES' Parents Bill of Rights for Data Privacy and Security, a copy of which has been signed by the Vendor and is set forth below.

Additional elements of Vendor's Data Security and Privacy Plan are as follows:

(a) In order to implement all state, federal, and local data security and privacy requirements, including those contained within this Data Sharing and Confidentiality Agreement, consistent with Erie 1 BOCES' data security and privacy policy, Vendor will: Review its data security and privacy policy and practices to ensure that they are in conformance with all applicable federal, state, and local laws and the terms of this Data Sharing and Confidentiality Agreement. In the event Vendor's policy and practices are not in conformance, the Vendor will implement commercially reasonable efforts to ensure such compliance.

(b) In order to protect the security, confidentiality and integrity of the Protected Data that it receives under the MLSA, Vendor will have the following reasonable administrative, technical, operational and physical safeguards and practices in place throughout the term of the MLSA: *See Exhibit E for Vendor Data Security and Privacy Plan*

(c) Vendor will comply with all obligations set forth in Erie 1 BOCES' "Supplemental Information about the MLSA" below.

(d) For any of its officers or employees (or officers or employees of any of its subcontractors or assignees) who have access to Protected Data, Vendor has provided or will provide training on the federal and state laws governing confidentiality of such data prior to their receiving access, as follows: Annually, Vendor will require that all of its employees (or officers or employees of any of its subcontractors or assignees) undergo data security and privacy training to ensure that these individuals are aware of and familiar with all applicable data security and privacy laws.

(e) Vendor [*check one*] __ √__ will___ will not utilize sub-contractors for the purpose of fulfilling one or more of its obligations under the MLSA. In the event that Vendor engages any subcontractors, assignees, or other authorized agents to perform its obligations under the MLSA, it will require such subcontractors, assignees, or other authorized agents to

execute written agreements as more fully described in Erie 1 BOCES' "Supplemental Information about the MLSA," below.

(f) Vendor will manage data security and privacy incidents that implicate Protected Data, including identifying breaches and unauthorized disclosures, and Vendor will provide prompt notification of any breaches or unauthorized disclosures of Protected Data in accordance with Section 6 of this Data Sharing and Confidentiality Agreement.

(g) Vendor will implement procedures for the return, transition, deletion and/or destruction of Protected Data at such time that the MLSA is terminated or expires, as more fully described in Erie 1 BOCES' "Supplemental Information about the MLSA," below.

5. Additional Statutory and Regulatory Obligations

Vendor acknowledges that it has the following additional obligations with respect to any Protected Data received from Participating Educational Agencies, and that any failure to fulfill one or more of these statutory or regulatory obligations shall be a breach of the MLSA and the terms of this Data Sharing and Confidentiality Agreement:

(a) Limit internal access to education records to those individuals that are determined to have legitimate educational interests within the meaning of Section 2-d and the Family Educational Rights and Privacy Act (FERPA).

(b) Limit internal access to Protected Data to only those employees or subcontractors that need access in order to assist Vendor in fulfilling one or more of its obligations under theMLSA.

(c) Not use education records for any purposes other than those explicitly authorized in this Data Sharing and Confidentiality Agreement.

(d) Not disclose any personally identifiable information to any other party, except for authorized representatives of Vendor using the information to carry out Vendor's obligations under the MLSA, unless:

(i) the parent or eligible student has provided prior written consent; or
(ii) the disclosure is required by statute or court order and notice of the disclosure is provided to Participating Educational Agency no later than the time of disclosure, unless such notice 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 that complies with Section 2-d, as more fully set forth in Erie 1 BOCES' "Supplemental Information about the MLSA," below.

(g) Provide notification to Erie 1 BOCES (and Participating Educational Agencies, to the extent required by, and in accordance with, Section 6 of this Data Sharing and Confidentiality Agreement) of any breach of security resulting in an unauthorized release of Protected Data by Vendor or its assignees or subcontractors in violation of state or federal law or other obligations relating to data privacy and security contained herein.

(h) Promptly reimburse Erie 1 BOCES, another BOCES, or a Participating School District for the full cost of notification, in the event they are required under Section 2-d to notify affected

parents, students, teachers or principals of a breach or unauthorized release of Protected Data attributed to Vendor or its subcontractors or assignees.

6. Notification of Breach and Unauthorized Release

(a) Vendor shall promptly notify Erie 1 BOCES of any breach or unauthorized release of Protected Data in the most expedient way possible and without unreasonable delay, but no more than seven (7) calendar days after Vendor has discovered or been informed of the breach or unauthorized release.

(b) Vendor will provide such notification to Erie 1 BOCES by contacting Michelle Okal-Frink directly by email at mokal@e1b.org, or by calling (716) 821-7200 (office) or (716) 374-5460 (cell).

(c) Vendor will cooperate with Erie 1 BOCES and provide as much information as possible directly to Michelle Okal-Frink or her designee about the incident, including but not limited to: a description of the incident, the date of the incident, the date Vendor discovered or was informed of the incident, a description of the types of personally identifiable information involved, an estimate of the number of records affected, the Participating Educational Agencies affected, what the Vendor has done or plans to do to investigate the incident, stop the breach and mitigate any further unauthorized access or release of Protected Data, and contact information for Vendor representatives who can assist affected individuals that may have additional questions.

(d) Vendor acknowledges that upon initial notification from Vendor, Erie 1 BOCES, as the educational agency with which Vendor contracts, has an obligation under Section 2-d to in turn notify the Chief Privacy Officer in the New York State Education Department ("CPO"). Vendor shall not provide this notification to the CPO directly. In the event the CPO contacts Vendor directly or requests more information from Vendor regarding the incident after having been initially informed of the incident by Erie 1 BOCES, Vendor will promptly inform Michelle Okal-Frink or her designees.

(e) Vendor will consult directly with Michelle Okal-Frink or her designees prior to providing any further notice of the incident (written or otherwise) directly to any other BOCES or Regional Information Center, or any affected Participating Educational Agency.

EXHIBIT D (CONTINUED)

SUPPLEMENTAL INFORMATION

ABOUT THE MASTER LICENSE AND SERVICE AGREEMENT
BETWEEN
ERIE 1 BOCES AND XSEL LABS, INC

Erie 1 BOCES has entered into a Master License and Service Agreement ("MLSA") with xSEL Labs, Inc. which governs the availability to Participating Educational Agencies of the following Product(s):

The SELweb suite, https://www.selweb.com/ - SELweb EE, SELweb LE, SELweb MS, SELweb HS; including, in addition to student competency measures, School Climate Survey Module and Adult SEL Competency Survey

Pursuant to the MLSA, Participating Educational Agencies may provide to Vendor, and Vendor will receive, personally identifiable information about students, or teachers and principals, that is protected by Section 2-d of the New York State Education Law ("Protected Data").

Exclusive Purpose for which Protected Data will be Used: The exclusive purpose for which Vendor is being provided access to Protected Data is to provide Participating Educational Agencies with the functionality of the Product(s) listed above. Vendor agrees that it will not use the Protected Data for any other purposes not explicitly authorized in the MLSA. Protected Data received by Vendor, or any of Vendor's subcontractors, assignees, or other authorized agents, will not be sold, or released or used for any commercial or marketing purposes.

Oversight of Subcontractors: In the event that Vendor engages subcontractors, assignees, or other authorized agents to perform one or more of its obligations under the MLSA (including any hosting service provider), it will require those to whom it discloses Protected Data to execute legally binding agreements acknowledging the obligation under Section 2-d of the New York State Education Law to comply with the same data security and privacy standards required of Vendor under the MLSA and applicable state and federal law. Vendor will ensure that such subcontractors, assignees, or other authorized agents abide by the provisions of these agreements by:

xSEL Labs has entered into a Data Privacy Agreement with 3-C Institute that acknowledges the obligation under Section 2-d of the New York State Education Law to comply with the same data security and privacy standards required of Vendor under the MLSA and applicable state and federal law. A copy of our agreement with 3-C Institute is available upon request.

Duration of MLSA and Protected Data Upon Expiration:

- The MLSA commences on March 29, 2022 and expires on June 30, 2025.
- Upon expiration of the MLSA without renewal, or upon termination of the MLSA prior to expiration, Vendor will securely delete or otherwise destroy any and all Protected Data remaining in the possession of Vendor or its assignees or subcontractors or other authorized persons or entities to whom it has disclosed Protected Data. If requested by Erie 1 BOCES and/or any Participating Educational Agency, Vendor will assist a Participating Educational Agency in exporting all Protected Data previously received back to the Participating Educational Agency for its own use, prior to deletion, in such formats as may be requested by the Participating Educational Agency.

EXHIBIT D (CONTINUED)

PARENTS BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY

Erie 1 BOCES is committed to protecting the privacy and security of student, teacher, and principal data. In accordance with New York Education Law § 2-d, the BOCES wishes to inform the community of the following:

(1) A student's personally identifiable information cannot be sold or released for any commercial purposes.

(2) Parents have the right to inspect and review the complete contents of their child's education record.

(3) State and federal laws protect the confidentiality of personally identifiable information, and 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.

(4) A complete list of all student data elements collected by the State is available for public review at http://www.nysed.gov/data-privacy-security/student-data-inventory, or by writing to the Office of Information & Reporting Services, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, New York 12234.

(5) Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed in writing to the Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, New York 12234. Complaints may also be submitted using the form available at the following website http://www.nysed.gov/data-privacy-security/report-improper-disclosure.

BY THE VENDOR:

Clark McKown (Apr 12, 2022 15:25 CDT)

_____

Signature

___**Clark McKown**_____

Printed Name

_____**Founder and President**___

Title

Apr 12, 2022

_____

Date

- In the event the Master Agreement is assigned to a successor Vendor (to the extent authorized by the Master Agreement), the Vendor will cooperate with Erie 1 BOCES as necessary to transition Protected Data to the successor Vendor prior to deletion.
- Neither Vendor nor any of its subcontractors or other authorized persons or entities to whom it has disclosed Protected Data will retain any Protected Data, copies, summaries or extracts of the Protected Data, or any de-identified Protected Data, on any storage medium whatsoever. Upon request, Vendor and/or its subcontractors or other authorized persons or entities to whom it has disclosed Protected Data, as applicable, will provide Erie 1 BOCES with a certification from an appropriate officer that these requirements have been satisfied in full.

Challenging Accuracy of Protected Data: Parents or eligible students can challenge the accuracy of any Protected Data provided by a Participating Educational Agency to Vendor, by contacting the student's district of residence regarding procedures for requesting amendment of education records under the Family Educational Rights and Privacy Act (FERPA). Teachers or principals may be able to challenge the accuracy of APPR data provided to Vendor by following the appeal process in their employing school district's applicable APPR Plan.

Data Storage and Security Protections: Any Protected Data Vendor receives will be stored on systems maintained by Vendor, or by a subcontractor under the direct control of Vendor, in a secure data center facility located within the United States. The measures that Vendor will take to protect Protected Data include adoption of technologies, safeguards and practices that align with the NIST Cybersecurity Framework and industry best practices including, but not necessarily limited to, disk encryption, file encryption, firewalls, and password protection.

Encryption of Protected Data: Vendor (or, if applicable, its subcontractors) will protect Protected Data in its custody from unauthorized disclosure while in motion or at rest, using a technology or methodology specified by the secretary of the U.S. Department of HHS in guidance issued under Section 13402(H)(2) of P.L. 111-5.

Exhibit E: SELweb Data Security and Privacy Plan

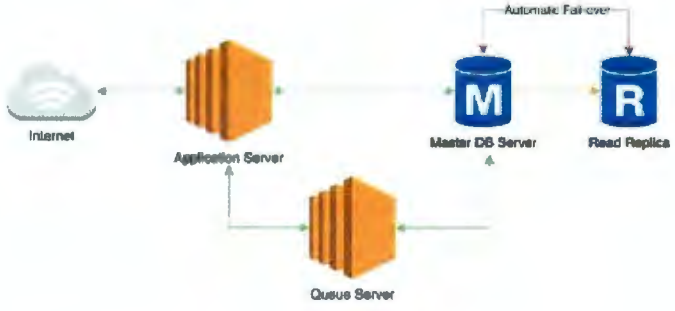
1. **Single Sign-On**: xSEL Labs currently offers SSO options through Clever and ClassLink.
2. **Scheduled maintenance:** Scheduled maintenance such as patch releases will be scheduled outside of school day hours of operation and therefore outside of assessmenthours of operation. Authentication services will not be affected by automatic maintenance. In the unlikely event that authentication services would need to be pausedfor maintenance, xSEL Labs will issue a memo for scheduled outage to CPS via email.
3. **Security protections are in place to keep systems updated based on industry standards (NIST, ISO, SOC, etc):** Infrastructure is patched and updated regularly, and in most cases, automatically. Policies are based on the NIST Cybersecurity Frameworkmodel and include risk assessment and management strategies, access control and preventative technologies, and continuous monitoring systems.
4. **There is state-of-the-indusfry encryption for PII data in motion and at rest:** Data inflight is secured by SSL/TLS encryption. Data at rest is stored using a combination of KMS/AES 256 encryption methods.
5. **xSEL Labs' project management methodology and how is it utilized to manage the implementation of the new services: which include scope, budget, communication, risk, and schedule management.** xSEL Labs uses the Kanban method to design, manage, and improve work flows.
6. **Support systems and qualified staff are in place to guide implementation, migration, transition and operations support:** Technical customer support is providedby xSEL Labs' implementation team. Once student rosters have been processed into SELweb, they are subjected to a Quality Assurance checklist by the xSEL Labs Implementation Team verifying 1) assignment plans have been defined correctly, 2) students and teachers have been populated into classes accurately, 3) date of births andgrade level data is verified, and 4) school level admins have been processed into SELweb and activation emails are scheduled. xSEL Labs uses Salesforce Service Cloudto manage customer case tracking, resolution, and communications.
7. **xSEL Labs quickly resolves issues as they arise, and formally provides a SLA, as well as documented remediation process for handling issues:** Issues that arise during active assessment are responded to immediately by the Implementation team to acknowledge they have been received and are being investigated. Common occurrences will be addressed immediately. And all issues are investigated to produce aroot cause. A summary of the root cause and actions taken to prevent a future occurrence are provided. Service's Service Level Agreement is provided to all customers.
8. **Systems are tested for readiness through a documented test plan:** School IT teamswill ensure that their devices support Firefox or Chrome 2018 or later and that their localinternet bandwidth can accommodate 2 mbps per student times the number of students they plan to assess simultaneously. They will register SELweb whitelist settings with thelocal Firewall and will visit this test website: https://www.selweb.com/test The test website verifies that images and audio files are permitted by the firewall as well as checks local bandwidth. School IT teams coordinate with xSEL Labs Implementation

team to run a QA test ensuring that Clever or ClassLink SSO is set up and functional bylogging in as several students through their accounts (when applicable).

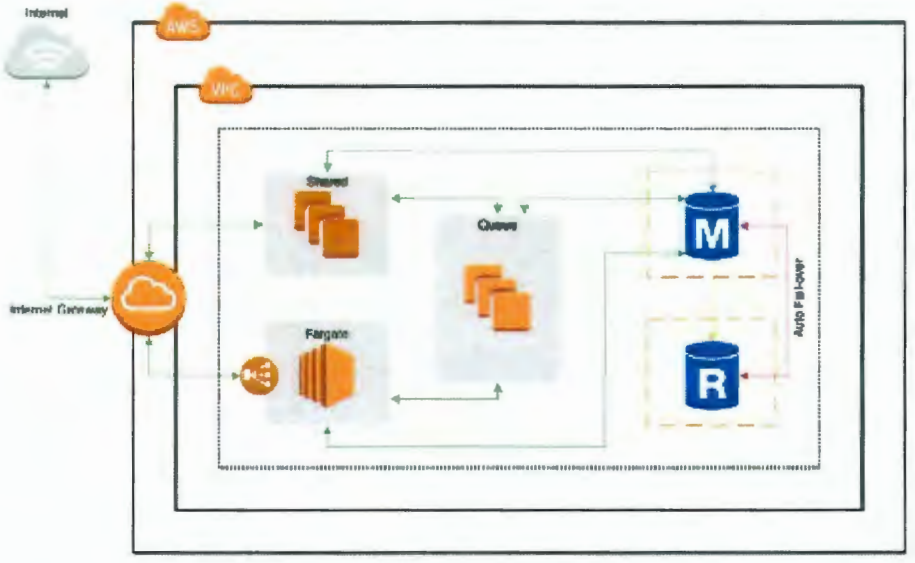
9. **Technical diagrams showing technical architecture, all data field requirements, and application and data flows for all IT services:** 3C's applications are deployed using managed automation processes, to cloud-based infrastructure architected to besecure, highly-available, and fault-tolerant. For most of our applications, we utilize a type of OS-level virtualization that allows us to run fully functioning and self-containedinstances that are immutable and logically isolated from each other.

   Data is stored in databases that are synchronously replicated into clusters that span multiple "availability zones" or unique physical locations within a specific geographic region. Using state-of-the-art failover technology, if one of the master database serversfail the replica server is automatically promoted to master while the failed instance is decommissioned and replaced as a new replica. Additionally, because our application and Web servers are deployed using OS-level virtualization, we take advantage of the technology's self-healing functionality that will restart/replace failed instances automatically. Some of our higher traffic or resource intensive applications are taken a step further by utilizing application load balancing and instance auto-scaling. This technology allows us to automatically scale our applications' footprint based on various metric data points such as traffic, CPU, and memory utilization.

   Simplified Infrastructure Diagram: End-users traverse the Internet to the server that the Application lives on. The Application interfaces directly with the Database server. The Application will offload certain tasks to be performed by the Queue server which also interfaces directly with the Database server. The Database server is configured in a highly-available and fault-tolerant manner where it synchronously mirrors itself to a Replica. Should there be a failure on the Master, the failing Master is removed, the Replica is automatically promoted to Master, and a new Replica is generated.



Advanced Infrastructure Diagram: End-users traverse the Internet to the AWS network. Traffic isthen routed to the Virtual Private Cloud through a device called an Internet Gateway. For applications that are deployed into the Shared environment, Operating System-level routing is performed to direct traffic to the specific Application. For applications that are deployed into the Fargate environment, traffic is directed to a Load-Balancer which routes the end-user to an instance running in an Auto-Scaling Cluster. The Auto-Scaling Cluster automatically scales based on demand and resource utilization. For both environments, the Application interfaces directly with the Database server. The Application will offload certain tasks to be performed by the Queueserver which also interfaces directly with the Database server. The Database server is configuredin a highly-available and fault-tolerant manner where it synchronously mirrors itself to a Replica. Should there be a failure on the Master, the failing Master is removed, the Replica is automatically promoted to Master, and a new Replica is generated.



10. **Disaster Recovery Provisions:** 3C's Web-based applications and sites are deployed toAmazon Web Services; a Cloud Service Provider by Amazon. All applications and sites are deployed in a Virtual Private Cloud, utilizing both public and private subnets for secure network communication, firewall rules called Security Groups that block unapproved port access, and various deployment strategies to maximize availability, fault-tolerance, and security.

    Network Infrastructure: Our Virtual Private Cloud (VPC) is built specifically for the hosting and management of applications and sites developed internally for 3C and its customers. This VPC isolates our infrastructure from other AWS customers' resources,ensuring that no external entity has direct access to 3C assets. Our Virtual Private

    Cloud is located in an AWS "Region" that is physically located somewhere in Ohio, USA.Inside this region, there are multiple geographically separate data-centers called "Availability Zones". To ensure our network infrastructure and servers/services are built for high-availability, we provision them across multiple Availability Zones within the Region so that if there were a catastrophic failure at a data-center, the applications and sites would continue to function. 3C's entire Virtual Private Cloud is built programmatically and can be rebuilt in any Region in AWS' quickly and with very little effort.

Compute: Applications are deployed using various strategies depending on their operational and traffic requirements. All applications are deployed using a stateless virtualization technology that allows for rapid recovery should there be a failure at the application layer. Some applications that require more resources or expect higher traffic,are deployed into load-balanced, auto-scaling clusters that will automatically scale up and down based on load, even repairing itself without the need for human or manual intervention. Application and site deployments have been standardized using automation tools and can be redeployed extremely quickly should the need arise.

Database: All application and site databases reside on servers that are part of a clusterthat spans multiple Availability Zones (Multi-AZ) for high-availability and consist of a primary server with synchronous replication to a replica. Should a failure arise, the underlying software for our database services will automatically, without human interaction, fail-over; promoting the replica to primary, decommissioning the previous primary instance, and generate a new replica based on the new primary instance.
Server-wide snapshots are taken multiple times per day and offer 3C the ability to restore to a particular point in time. Additionally, individual database backups are takennightly and stored for extended periods of time.

Storage: Files, backups, and static content served by a Content Delivery Network (CDN)are all stored in AWS' storage service called S3. All objects stored in S3 are guaranteedby AWS' SLA and in the case of CDN hosted files, are replicated and distributed throughout edge locations all over the world ensuring the fastest delivery to the end- users' initiating request.

11. **Data Management allows for centralized management and integrations.** SELweb supports CSV upload of student, teacher, and administrator rosters. These uploads use field names and field value formats aligned with the OneRoster IMS Global interoperability standard for roster synchronization. SELweb also supports CSV export of student scores in a standard format which could be used in an integration of collected data.