



Central Susquehanna  
Intermediate Unit

**Exhibit 1.a**  
**Central Susquehanna Intermediate Unit**  
**Computer Service Rates 2024-2025 – Financials/Tax only**  
 School entity only (not applicable to IU, AVTS/technical institute or government agency)

<b>CHECK ✓ SERVICES</b>	<b>APPLICATION</b>	<b>BILLING BASIS PER UNIT</b>	<b>ANNUAL RATE</b>	<b>ANNUAL MINIMUM</b>	<b>CLASS</b>
<input type="checkbox"/>	Assets Inventory	Flat fee, plus per student on file  First 2,000 students 2,001 – 4,000 students 4,001 – 7,499 students Over 7,500 students	\$125  \$1.17 0.59 0.00 0.30	\$1,800	C
<input type="checkbox"/>	Bidding	Flat fee, plus per student on file  First 2,000 students 2,001 – 4,000 students 4,001 – 7,499 students Over 7,500 students	\$375  \$1.19 0.60 0.00 0.31	\$1,800	C
<input checked="" type="checkbox"/>	Fund Accounting (includes GL, AP, AR, POs and Budget Prep)	Flat fee, plus per student on file  First 1,500 students 1,501 – 4,000 students 4,001 – 7,499 students Over 7,500 students	\$780  \$4.51 2.26 0.00 1.09	\$2,200	A
<input checked="" type="checkbox"/>	Human Resources* (Previously identified as Personnel)	Flat fee, plus per student on file  First 2,500 students 2,501 – 4,000 students 4,001 – 7,499 students Over 7,500 students	\$500  \$2.40 1.19 0.00 0.59	\$1,975	B
<input checked="" type="checkbox"/>	Payroll*	Flat fee, plus per student on file  First 2,000 students 2,001 – 4,000 students 4,001 – 7,499 students Over 7,500 students	\$500  \$5.22 2.52 0.00 1.21	\$2,200	A

\* Staff Portal included with purchase of Human Resources/Payroll applications



Central Susquehanna  
Intermediate Unit

CHECK ✓ SERVICES	APPLICATION	BILLING BASIS PER UNIT	ANNUAL RATE	ANNUAL MINIMUM	CLASS
<input type="checkbox"/>	Interim Tax Billing	Included in Tax Billing; call for pricing if you do not use Tax Billing	N/A	N/A	C
<input type="checkbox"/>	Tax Billing – standard Tax Billing – mailers	Flat fee, plus per bill on file	\$225	\$1,875	C
<input checked="" type="checkbox"/>		Per bill Per bill	\$0.34 0.41**		
<input checked="" type="checkbox"/>	Tax Collection	Flat fee, plus per taxables on file	\$225	\$1,675	C
		First 50,000 taxables Above 50,000 taxables	\$0.21 0.10		

\*\* Plus, flat forms handling charge of \$350 and "then-current" standard postage rate per mailer

- Payroll check history and Fund Accounting detailed transaction data will be maintained for seven calendar or fiscal years, respectively. CSIU reserves the right to purge any Payroll history or to summarize Fund Accounting transactions more than seven years old at any time.
- All **training** at the CSIU (including webinars), within reason, is available at no charge. All on-site training, on-site support, and travel time is billable at the CSIU then-current hourly rate. Phone training is available at no charge but is distinguished from phone support by being pre-scheduled and of at least one hour in length.
- Training for web-enabled modules or teachers (e.g., Employee or Vendor Portals, teachers entering requisitions) is conducted for trainers who will be training those back at the client site. This training falls into the same guidelines as above, however if individual users attend the training, they will be charged the standard rate.
- Class determines the amount of annual, non-billable, phone support time for an application: class A includes 12 hours of phone support; B includes 8 hours; and C includes 4 hours. Billing for phone support in excess of these included hours will be at the then-current hourly rate.
- One hour of miscellaneous phone support time (not related to a specific application, such as technical or security issues) will be allowed per application that is implemented by January 1 of the fiscal year.
- Charges are calculated based upon the most recent audited PIMS enrollment totals, posted on the PDE website. Excess support, data conversions, and onsite training are billed monthly at \$97/hour. Consulting and staff augmentation are billable at \$120/hour. Custom programming, if approved, is billed at \$134/hr. Travel time is billable at the same rate as the service rendered. Note: minimums will only be prorated on a half-year basis. i.e., installations from July to December are full price...installations from January to June half price.
- For **NEW CLIENT IMPLEMENTATIONS**: There is a one-time flat setup fee of \$350/per non-tax application (e.g., excludes Tax Billing and Tax Collection)



**Central Susquehanna  
Intermediate Unit**

- Data transfers for tax applications are billable at \$450 for each occurrence (e.g., tax collection data from outside vendors, and the transfer of tax billing data from CSIU servers to an external server). Please call for additional tax bill related options and pricing.
- The CSIU is responsible for regularly backing up files, moving the back-up media to an off-site facility, and, if necessary, restoring files to the best of its ability.
- Services do not include any form of paper, labels, checks, envelopes, special forms or printing services.
- Please contact CSIU for pricing confirmation if your district enrollment exceeds the upper limits in the Billing Basis per Unit column or if you plan on implementing CSIU applications mid-year (fees & associated support hours are prorated).

Signature of client representative below indicates agreement with all the above specified conditions.

SIGNATURE: \_\_\_\_\_

TITLE: \_\_\_\_\_

PRINT NAME: \_\_\_\_\_

EMAIL: \_\_\_\_\_

DISTRICT/AGENCY NAME: \_\_\_\_\_

DATE: \_\_\_\_\_



**Central Susquehanna  
Intermediate Unit**

**Exhibit 1.e  
Central Susquehanna Intermediate Unit  
Computer Service Rates 2024-2025 – SCView Document Management System  
LEA only (not applicable for government agency)\***

<b>CHECK ✓ SERVICES</b>	<b>APPLICATION</b>	<b>BILLING BASIS PER UNIT</b>	<b>ANNUAL RATE</b>	<b>ANNUAL MINIMUM</b>	<b>CLASS</b>
<input type="checkbox"/>	Document Management/ Electronic Forms Builder/ Workflow  (Includes unlimited user licenses)	Flat fee, plus per student on file  First 1,800 students 1,801 – 2,800 students 2,801 – 3,800 students 3,801 – 5,800 students 5,801 – 8,000 students Over 8,001 students	\$825  \$4.54 1.03 0.77 0.51 0.00 0.26	\$8,995	A
<input type="checkbox"/>	Document Management/ Electronic Forms Builder/ Workflow – LITE option  (LITE option only includes 3 user licenses)	Flat fee, plus per student on file  First 1,800 students 1,801 – 2,800 students 2,801 – 3,800 students 3,801 – 5,800 students 5,801 – 8,000 students Over 8,001 students	\$825  \$3.43 1.03 0.77 0.51 0.00 0.26	\$6,995	A
<input type="checkbox"/>	Purchasing / Accounts Payable  (includes 1 SCScan Station license)	Flat fee per student tier  0 – 1,800 students 1,801 – 2,800 students 2,801 – 3,800 students 3,801 – 4,800 students 4,801 – 8,000 students Over 8,001 students	\$1,995 \$2,495 \$2,995 \$3,495 \$3,995 \$4,495	\$1,995	B
<input type="checkbox"/>	Staff Onboarding	Flat fee per student tier  0 – 1,800 students 1,801 – 2,800 students 2,801 – 3,800 students 3,801 – 4,800 students 4,801 – 8,000 students Over 8,001 students	\$2,995 \$3,495 \$3,995 \$4,495 \$4,995 \$5,495	\$2,995	B
<input type="checkbox"/>	Mileage Reimbursement	Flat fee	\$695	\$695	C
Quantity: —	SCScan Station License	Flat fee	\$895	\$895	C



**Central Susquehanna  
Intermediate Unit**

\* Intermediate Unit student count based upon the average of all school districts within their boundary

- SCView® is a third-party product of SC Strategic Solutions (SCSS) for which CSIU assumes hosting, training, support and co-development responsibilities.
- The core Document Management system, Electronic Forms Builder module and Workflow module are packaged at one annual price. This also includes unlimited user accounts, creation of unlimited electronic forms and addition of 100,000 documents per year. Documents over 100,000 per year will be charged at .01/per document.
- Annual fees are calculated based upon the most recent audited PIMS enrollment totals, posted on the PDE website.
- All **training** at the CSIU (including webinars), within reason, is available at no charge. All on-site training, on-site support, and travel time is billable at the CSIU then-current hourly rate. Phone training is available at no charge, but is distinguished from phone support by being pre-scheduled and of at least one hour in length.
- Training for all modules is for trainers who will be training those back at the client site. This training falls into the same guidelines as above, however if individual users attend the training, they will be charged the standard rate.
- Class determines the amount of annual, non-billable, phone support time for a module: class A includes 12 hours of phone support; B includes 8 hours; and C includes 4 hours. Billing for phone support in excess of these included hours will be at the then-current hourly rate.
- One hour of miscellaneous phone support time (not related to a specific module, such as technical or security issues) will be allowed per Class A module that is implemented by January 1 of the fiscal year.
- Charges are calculated based upon the most recent audited PIMS enrollment totals, posted on the PDE website. Excess support, onsite training, and electronic forms development is billed monthly at \$97/hour. Consulting is billable at \$120/hour. Custom programming, if approved, is billed at \$134/hr. Travel time is billable at the same rate as the service rendered.
- The CSIU will build up to two electronic form templates, at no additional cost, upon implementation of the SCView system. Requests for CSIU to build additional electronic forms templates are billed monthly at \$97/hour.
- If you plan on implementing SCView mid-year, fees & associated support hours may be prorated. Please contact CSIU for pricing confirmation. Note: minimums will only be prorated on a half-year basis. i.e. installations from July to December are full price...installations from January to June half price.
- Data conversion of documents are billed at \$97/hour, plus \$.01 (one cent) per document converted.
- The CSIU is responsible for regularly backing up files, moving the back-up media to an off-site facility, and, if necessary, restoring files to the best of its ability.



**Central Susquehanna  
Intermediate Unit**

- For purposes of obtaining the benefit of the Services only, SCSS grants to Customer a non-exclusive, non-transferable license to use the related software for internal purposes only. Customer shall not modify, decompile, disassemble, reverse engineer or attempt to reconstruct, reconfigure or develop derivative works based upon any of the computer hardware, equipment or software utilized by SCSS.
- CSIU and SCSS shall not be responsible for misfiled documents within the records provided for scanning/imaging, nor for any inaccurate or incorrect information contained in records received from Customer.

Signature of client representative below indicates agreement with all of the above specified conditions.

SIGNATURE: \_\_\_\_\_

TITLE: \_\_\_\_\_

NAME: \_\_\_\_\_

EMAIL: \_\_\_\_\_

DISTRICT/AGENCY NAME: \_\_\_\_\_

DATE: \_\_\_\_\_

# Exhibit 2 - CSIU

## Application Service Provider Information Security Specifications

---

Provider Location: CSIU Main Office, 90 Lawton Lane, Milton, PA 17847  
Client Representatives: CSIU Computer Services Staff

### 1. Physical controls in place for security assurance

- a. Hosted systems are maintained in our data center.
- b. Access to the data center is monitored electronically. Personnel entering the room without electronic passes are admitted only by authorized personnel. Additionally, the data center is located behind secured doors in a passage designated for CSIU personnel only. Finally, all entrances to the building are monitored electronically, by camera, and by front desk personnel, thus presenting four levels of security.
- c. Staff access to the application servers and software is restricted to a separate domain than CSIU staff. Temporary access to client data is granted to staff on an 'as needed' basis for resolving client-initiated calls. This access to client data automatically "times-out" at the end of an established access period, and is unique to each request; hence, an audit trail is established. Also, these occurrences are documented regarding need, date, and time.
- d. The datacenter is equipped with smoke detectors and an automatic fire suppression system (HFC-125 Extinguishing System). The system is interconnected and monitored by a third-party alarm company which reports incidents to the Union County 911 Center as needed. There is also air conditioning with a second back-up unit.
- e. The entire main CSIU office is supported by a diesel generator that comes on-line, within seconds, in the event of a power outage. This generator can provide the full electrical capacity for the facility and can run for multiple days at a time if there is diesel fuel available. Weekly tests are completed to ensure this generator is in proper working order.

### 2. Security Safeguards based on auditor recommendations

#### a. Security Protocols for Windows Servers:

- User accounts are locked after three incorrect login attempts and must be unlocked manually by an authorized staff member.
- User passwords must be changed every 30 days.
- The minimum length of any password is eight characters and must include three of the four categories: uppercase letters (A-Z), lowercase letters (a-z), numeric (0-9), or special characters (for example, !\$,%,&).
- The system logs the previous ten passwords for each user, requiring that none of the previous ten passwords can be repeated.
- Accounts that are inactive for more than 3 months are disabled and only re-enabled upon client request.
- Clients logged into a session that remains inactive (no keyboard or mouse activity) for more than 60 minutes will be logged off.

**b. Web-Based Student Information System (SIS)**

- Clients logged into a session that remains inactive (no page updates) for more than 60 minutes will be logged off automatically.
- User accounts are locked after three incorrect login attempts and must be unlocked manually by an authorized staff member.
- Agency system administrator can set the frequency of expiration; every 7 days, 30 days, 60 days, or 90 days, or choose not to enforce expiration.
- The minimum length of any password is eight characters and must include one number (0-9) or a special character (for example, !\$,%,#).

**c. Web-Based Financial Information System (FIS)**

- Clients logged into a session that remains inactive (no page updates) for more than 30 minutes will be logged off automatically.
- User passwords must be changed every 30 days.
- User accounts are locked after three incorrect login attempts until unlocked or 10 minutes passes.
- The minimum length of any password is eight characters and must include three of the four categories: uppercase letters (A-Z), lowercase letters (a-z), numeric (0-9), or special characters allowed are (&!@#\$\$%^+=).
- The system logs the previous ten passwords for each user, requiring that none of the previous ten passwords is repeated.

**3. Single-Sign-On (SSO) - available for FIS clients**

- Authentication can be shifted from the FIS to an external provider of the agency's choice.
- Using this service requires the agency to assume additional responsibilities and oversight. It is *critical* that agencies are aware of their responsibility for controlling access to the FIS logins and password complexity/change requirements, which under this method is no longer within CSIU's purview for strict authentication control.
- All SSO FIS solutions require a secure internet connection using client/server certificates to connect to the client's authentication service.
- It that are external to the CSIU (e.g., problems with connectivity to or failure of the external authentication service) can mean users will not be able to log in to their respective FIS website at CSIU. CSIU will be glad to assist in troubleshooting to confirm the source of any disruption, failure, and disconnect.
- Any audit inquiries or questions regarding SSO rules administered by an agency not using the FIS out-of-the-box security (as described in 2c above) will be redirected to the agency's administration.



## 4. Data Confidentiality, Integrity and Availability

### a. Confidentiality

- All eService websites require client web browsers to connect at a minimum using a 256-bit encryption certificate (SSL) in all connections.
- CSIU uses Microsoft Active Directory security protocols and deploys current security patches and service packs. Client data is segmented in a separate Active Directory domain.
- Users are logged out of web sessions after 20 minutes of inactivity, except for the SIS which allows up to 60 minutes of inactivity.
- Data is located on servers housing other client data. Client data is secured via Microsoft's NTFS and Microsoft SQL Server permissions; thus, prohibiting one client access to another client's data.
- CSIU staff are required to read and sign a job description which includes the following language: *"The person employed in this position shall maintain confidentiality with regard to the personal and private information about clients and coworkers, programs and services and any other proprietary information accrued as a result of CSIU employment or as required by state or federal laws and regulations."*
- In response to client requests to investigate software malfunctions and data corruption, employees and agents of the CSIU may need to review client data. The CSIU acknowledges this data is confidential and is bound to maintain the confidentiality of the data to the extent that it can be maintained given the nature of the client's request for support.
- The CSIU will not disclose or re-disclose the personally identifiable information from student and confidential records that it receives to any other party without the prior consent of the staff, parent, or eligible student, and the CSIU will use the personally identifiable information that it receives only for the purpose for which the disclosure to the CSIU was made.
- A complete vulnerability assessment and penetration test has been performed by the PA National Guard. We have developed a good relationship with their team and continue to utilize their services ongoing.
- Weekly vulnerability scans are completed via the NCATS program, offered by DHS through US-CERT. A thorough report is reviewed with our internal teams weekly.
- CSIU is a member of the Multi-State Information Sharing and Analysis Center® (MS-ISAC®), which is funded and sponsored by the US Department of Homeland Security. We continually adjust our security priorities as needs are presented by this organization.

### b. Integrity

- Backups
  - i. All data (VM and file-level) is encrypted and backed up to local storage daily and database logs are backed-up hourly.

- ii. Daily all data and servers are backed-up with an industry leading enterprise backup software company off-site in an encrypted repository 80 miles away from CSIU's main data center.
  - iii. A full cycle of a minimum of 30-days of back-ups are retained for additional protection along with snapshots of the backup data.
- We institute change management procedures designed to ensure continued data integrity for client data.
  - i. Updates that are applied are completed in a test/QA environment before we move them to production.
  - ii. Application changes that go outside of our normal update sequences must have management authorization before being completed in a production environment.
  - iii. Our processes are limited to specific approved administrators to ensure rogue changes or updates do not happen
- CSIU staff are not permitted to change client data without signed authorization from an approved client contact.

c. Availability

- Disaster Recovery
  - i. No matter how much planning and proactivity is done, there is always a chance for disaster to strike. We have taken measures to be ready for situations involving lengthy outages in our disaster recovery strategy.
  - ii. We have a fully redundant data center which is replicated 80 miles away from CSIU's main data center. In the case of disaster or very extended outage, we can failover operations to the redundant location. We are continuing to enhance these capabilities ongoing.
  - iii. This plan is practiced regularly, and we strive to improve our recovery point objective (RPO) in findings during our practice scenarios.
  - iv. A copy of the full CSIU Computer Services Disaster Recovery Plan is available for review at our central office. Please contact our technical support staff if you have additional questions.
- Virtualization
  - i. We cluster our VM's which are highly available, and load balanced across multiple cluster hosts
  - ii. We use a storage area network (SAN) containing SSD hard drives which are RAID protected and use a 10G Base-T network backend to ensure high read/write speeds (IOPS) to our compute infrastructure.
  - iii. In the case of equipment malfunction or failure, our virtualization clusters are sized appropriately to ensure we have capacity to resume operations rapidly.
- CSIU pushes for continuous quality improvement by monitoring and anticipating problems **before** services are disrupted, whenever possible.
  - i. Automatic tests on hundreds of established metrics are running 24/7. When defined thresholds are met, notifications are sent via email and text alerts to

CSIU technical support staff for resolution; new metrics are added continuously to be proactive.

- ii. If there is a service disruption, CSIU keeps clients informed by using a public website (<https://csiu.statuspage.io>) to post service status information. Clients are encouraged to subscribe to emails and text messages posted by CSIU on this site to know about service issues or when upgrades are scheduled.
- We strive to maintain no single points of failure within our infrastructure. We have added additional redundancy wherever it is possible, to ensure this is possible. For example, we have instituted the following in our datacenter;
    - i. Redundant firewalls at our perimeter allowing for high availability failover
    - ii. Redundant switches in our core multi homed to lower-level switches
    - iii. Each physical server is doubly connected to separate Uninterruptible Power Supply (UPS) systems to carry through the gap from the loss of power until our building wide generator comes online.
    - iv. Dual ISP networks together provide redundancy in the event of an internet interruption.
    - v. All network traffic passes through our ISP network protection, and then through a route with an access-list limiting port access to all devices within our private network. Only approved devices have ports we specifically designate opened to the outside.

## **5. Hardware used by the client**

- Client hardware considerations are beyond CSIU control.
- Clients can access CSIU applications with a variety of operating systems and hardware through a standardized session
- Client web browsers must be able to support an SSL 256-bit encryption certificate to access CSIU web applications.
- We strongly suggest that client hardware accessing CSIU applications do not operate with administrator rights or without advanced endpoint protection installed.