



Privacy Impact Assessment (PIA)
for the

SecurityTouch Learning Management System

November 19, 2019

For PIA Certification Updates Only: This PIA was reviewed on **November 19, 2019** by **Deborah Coleman** certifying the information contained here is valid and up to date.

Contact Point

Contact Person/Title: Jamal Al-Faleh, Information System Security Officer
Contact Email: jamal.al-faleh@ed.gov

System Owner

Name/Title: Deborah Coleman
Principal Office: Office of the Chief Information Officer (OCIO)

Please submit completed Privacy Impact Assessments to the Privacy Office at privacysafeguards@ed.gov

Please complete this **Privacy Impact Assessment (PIA)** on how personally identifiable information (PII) is collected, stored, protected, shared, and managed electronically by your system. You may wish to consult with your ISSO in completing this document. **If a question does not apply to your system, please answer with N/A.**

1. Introduction

- 1.1. Describe the system including the name, acronym, and a brief description of the program or purpose for the system.

The SecurityTouch Learning Management System (STLMS) is used to provide mandatory cyber security and privacy awareness training and role-based training to users and to provide mandatory cyber security and privacy awareness training to new employees, interns and volunteers. STLMS tracks and reports on completed awareness and role-based training enabling the Department to meet quarterly and annual FISMA reporting requirements.

- 1.2. Describe the purpose for which the personally identifiable information (PII)¹ is collected, used, maintained or shared.

To comply with Federal laws and regulations, Agencies must provide initial, continuing, and refresher training at the awareness level, policy level, implementation level, and performance level for executives, program and functional managers, information resources managers, security and audit personnel, automated data processing management, operations, and programming staff, and end users. To comply with Federal law including FISMA, agencies must report to the Office of Management and Budget (OMB) and the Department of Homeland Security (DHS) on how effectively they are managing their security and privacy programs including data specific to the successful completion of required Cybersecurity Awareness and Role-based Training.

STLMS is used to provide mandatory cyber security and privacy awareness training and role-based training to users. STLMS tracks and reports on completed awareness and role-based training enabling the Department to meet quarterly and annual FISMA reporting requirements.

- 1.3. Is this a new system, or one that is currently in operation?

Currently Operating System

¹ The term “personally identifiable information” refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc. [OMB Circular A-130, page 33](#)

1.4. Is this PIA new, or is it updating a previous version?

Updated PIA

1.5. Is the system operated by the agency or by a contractor?

Contractor

1.5.1. If the system is operated by a contractor, does the contract or other acquisition-related documents include privacy requirements?

N/A

Yes

2. Legal Authorities and Other Requirements

If you are unsure of your legal authority, please contact your program attorney.

2.1. What specific legal authorities and/or agreements permit and regulate the collection and use of data by the system? Please include name and citation of the authority.

The legal authority to collect and use this data include the, Federal Information Security Modernization Act (FISMA) of 2014 (Title III of Public Law 107-347), OMB Circular A-130, Security of Federal Automated Information Resources, National Institute of Standards and Technology (NIST) Special Publication (SP) 800-16, Revision (Rev) 1, A Role - Based Model for Federal Information Technology / Cyber Security Training and NIST SP 800-50, Building an Information Technology Security Awareness and Training Program.

SORN

2.2. Is the information in this system retrieved by an individual's name or personal identifier such as a Social Security Number or other identification?

Yes

2.2.1. If the above answer is **YES**, this system will need to be covered by Privacy Act System of Records Notice(s) (SORN(s)).² Please provide the SORN name, number, Federal Register citation and link, or indicate that a SORN is in progress.

² A System of Records Notice (SORN) is a formal notice to the public that identifies the purpose for which PII is collected, from whom and what type of PII is collected, how the PII is shared externally (routine uses), and how to access and correct any PII maintained by ED. <https://connected.ed.gov/om/Documents/SORN-Process.pdf>

N/A

The Department will update this section to provide an applicable SORN.

2.2.2. If the above answer is **NO**, explain why a SORN was not necessary. For example, the information is not retrieved by an identifier, the information is not maintained in a system of records, or the information is not maintained by the Department, etc.

N/A

[Click here to enter text.](#)

Records Management

If you do not know your records schedule, please consult with your records liaison or send an email to RMHelp@ed.gov

2.3. What is the records retention schedule approved by National Archives and Records Administration (NARA) for the records contained in this system? Please provide all relevant NARA schedule numbers and disposition instructions.

The Department shall submit a retention and disposition schedule that covers the records contained in this system to the National Archives and Records Administration (NARA) for review. The records will not be destroyed until such time as NARA approves said schedule.

2.4. Is the PII contained in this system disposed of appropriately, and in accordance with the timelines in the records disposition schedule?

Yes

3. Characterization and Use of Information

Collection

3.1. List the specific PII elements (e.g., name, email, address, phone number, date of birth, Social Security, etc.) that the system collects, uses, disseminates, or maintains.

Data elements collected include the following: Title, first name, middle initial, last name, job role, company name, full address, phone number, time zone, Principal Office, email address, course name, training compliance status, training completion dates, and user status of an employee or contractor.

3.2. Does the system collect only the minimum amount required to achieve the purpose stated in Question 1.2?

Yes

3.3. What are the sources of PII collected (e.g., individual, school, another agency, commercial sources, etc.)?

A secure web form on the user registration page of the STLMS web application collects the personally identifiable information (PII) from STLMS users.

3.4. How is the PII collected from the stated sources listed in Question 3.3 (e.g., paper form, web page, database, etc.)?

A secure web form on the user registration page of the STLMS web application collects the personally identifiable information (PII) from STLMS users.

The SecurityTouch application functionality also includes an import feature which allows application administrators to efficiently create user accounts for employees and contractors by uploading a spreadsheet or comma separated values file containing the same PII data collected through the online user registration page. Additionally, training completion report data from the FedTalent system is imported into the SecurityTouch database to consolidate training completion tracking and reporting into a single system. In addition to the information collected during user registration, the FedTalent import also collects title, first name, middle initial, last name, job role, company name, full address, phone number, time zone, Principal Office, email address, course name, training compliance status, training completion dates, and user status of an employee or contractor. The information collected is not used to link or cross-reference multiple databases. The application administrators manually validates the PII data.

3.5. How is the PII validated or confirmed to ensure the integrity of the information collected?³ Is there a frequency at which there are continuous checks to ensure the PII remains valid and accurate?

A secure web form on the user registration page of the STLMS web application collects information from STLMS users. End user training profiles are accessible for validation by end users as well as Information System Security Officers (ISSOs) within each Principal Office, the Office of the Chief Information Officer (OCIO)/Information

³ Examples include restricted form filling, account verification, editing and validating information as it's collected, and communication with the individual whose information it is.

Assurance Services/Policy and Planning Branch personnel that manage the Department's cybersecurity training program, and contractor personnel that provide Help Desk support services for STLMS.

Use

3.6. Describe how the PII is used to achieve the purpose stated in Question 1.2 above.

The Department uses the information collected to create and update training accounts for end users, enroll end users into training courses, facilitate the completion of the training course(s), provide end users with completion certificates, communicate with end users, and track and report training completions and failures. In addition, the Department uses the information it collects from end users to confirm the individual's identity, establish their eligibility for system access, and to provide and monitor system security. Additionally, training completion data for Federal employees is imported from the Department of Interior's FedTalent into the STLMS database to consolidate all training records into a single system. This consolidation enables the Department to efficiently track and report training completions and failures as required to comply with mandated FISMA reporting.

PII collected or maintained by STLMS is not shared with outside of the Department. SecurityTouch does not utilize data mining to identify previously unknown patterns in the information collected and no tools are used to analyze or produce new data. It does not use commercial information or publicly available information.

3.7. Is the system using PII for testing/researching new applications or information systems prior to deployment or for training employees?

No

3.7.1. If the above answer is **YES**, what controls are in place to minimize the risk and protect the data?

N/A

Social Security Numbers

It is the Department's Policy that, in order to collect Social Security Numbers, the System Owner must state the collection is: 1) authorized by law, 2) necessary for an agency purpose, and 3) there is no reasonable alternative.

- 3.8. Does the system collect Social Security Numbers? Note that if the system maintains Social Security Numbers but does not explicitly collect them, answer 3.8.1 to address the purpose for maintaining them.

No

- 3.8.1. If the above answer is **YES**, explain the purpose for its collection, and how the SSN will be used.

N/A

- 3.8.2. Specify any alternatives considered in the collection of SSNs and why the alternatives were not selected.

N/A

4. Notice

- 4.1. How does the system provide individuals with notice about the collection of PII prior to its collection (e.g., direct notice, such as a Privacy Act Statement (if applicable) or public notice, such as a SORN, PIA,)? If notice is not provided, explain why not.

The Department provides notice of its information collection in several ways. First, notice is provided through this Privacy Impact Assessment. Secondly, the Department provides notice via a Privacy Act Statement, which is included on the SecurityTouch online user registration page. Finally, SecurityTouch states the privacy policy on a dedicated web page.

- 4.2. Provide the text of the notice or the link to the webpage where the notice is posted if notice is provided other than by SORN or PIA.

N/A

SecurityTouch Learning Management System Privacy Policy

Thank you for visiting the U.S. Department of Education (ED) SecurityTouch Learning Management System (STLMS) and reviewing our privacy policy. This privacy policy explains how the ED STLMS collects, uses, and discloses Personally Identifiable Information (PII) through this website, application services, or when you otherwise contact support. By accessing or using the STLMS application, you accept and agree to the terms of this privacy policy.

What PII Do We Collect?

On some of our web pages we offer interactive forms that let you voluntarily submit personal information to register for an account and complete cybersecurity and privacy awareness courses. We collect information you provide directly to us during the user registration process. This information includes your full name, email address, job role, company name, country, city, Department of Education Principal Office, and your security questions. Also, we record the names of the courses that you are assigned, training compliance status, and training completion dates.

When you access the STLMS application, we automatically record technical information. This information is recorded within the logs of the STLMS application. Specifically, this information includes the following: active sessions, access times, pages viewed, and your IP address.

If you send us an email, the message will usually contain your return email address. If you include PII in your email because you want us to address issues specific to your situation, we may use that information in responding to your request. Also, email is not necessarily secure against interception. Please send only information necessary to help us process your request.

How Do We Use PII?

As stated above, we collect PII necessary to provide, maintain, and improve the services that the STLMS application offers. Specifically, we use the PII that is collected to achieve the following: create and update training accounts for end users; enroll end users into ED mandatory cybersecurity and privacy awareness training courses; facilitate the completion of these training courses; provide end users with completion certificates; communicate with end users; and track and report training completions and failures. Also, PII is used to verify end users' identity; establish end users' eligibility for system access; and provide and monitor the security of the STLMS application. Information collected is shared internally with each ED Principal Office to ensure assigned users are in compliance with the Department's cybersecurity and privacy awareness training program requirements.

With Whom Do We Share PII?

Ultimately, PII that is collected and maintained by the STLMS application is not shared with any organization outside of the Department. The information that is shared internally is limited to the viewing of end users' training profiles and training completion reports; moreover, only authorized individuals (i.e. the Office of the Chief Information Officer (OCIO), Information Assurance Services (IAS), Governance, Risk and Policy Branch personnel, Information System Security Officers (ISSO) from each Principal Office, and the STLMS Helpdesk) are allowed to view the aforementioned information.

For How Long Do We Keep PII?

STLMS retains collected PII for as long as necessary for the purposes stated in this privacy policy or other legitimate business purposes, which include the obligations enforced by our legal or regulatory entities. We determine the appropriate retention period for PII based on the following: the amount, nature, and sensitivity of the PII; the potential risk from unauthorized use or disclosure of PII; whether we can achieve the purposes of the processing through other means; and the applicable regulatory obligations, legal requirements, and Department policy.

After the applicable retention period has expired, PII will be destroyed using approved data deletion standards. If there is any technical reason as to why we are unable to entirely delete PII from the STLMS application, then we will take additional measures to ensure that PII will not be used any further. For more information on applicable data retention periods, contact us by using the information provided in *Contact Us* section of this privacy policy.

Your Rights

Account Information

You may update and/or correct your PII at any time by logging into your online account and going to your profile page or emailing us at support@k2share.com. If you wish to delete or deactivate your account, then email us at support@k2share.com; however, it should be noted that we may retain certain information as required by law or for legitimate business purposes. Also, we may retain cached or archived copies of information about you for a certain period of time. For more information on data retention periods, contact us by using the information provided in *Contact Us* section of this privacy policy.

- 4.3. What opportunities are available for individuals to consent to uses (including new uses of previously collected PII), decline to provide PII, or opt out of the project?

The user has the option to opt out by declining to accept the Rules of Behavior; however, in doing so, the user will be unable to complete mandatory training and placed at risk of having his/her network account disabled.

- 4.4. Is the notice referenced in Question 4.1 reviewed and revised when there are changes in the practice, policy, or activities that affect the PII and privacy to ensure that individuals are aware of and can consent to, where feasible, these changes?

Yes

5. Information Sharing and Disclosures

Internal

5.1. Will PII be shared internally with other ED principal offices? If the answer is **NO**, please skip to Question 5.4.

Yes

5.2. What PII will be shared and with whom?

N/A

Access to view end user training profiles and training completion reports is limited to authorized Information System Security Officers (ISSOs) within each Principal Office, the Office of the Chief Information Officer (OCIO)/Information Assurance Services/Policy and Planning Branch personnel that manage the Department's cybersecurity training program, and contractor personnel that provide Help Desk support services for SecurityTouch.

5.3. What is the purpose for sharing the specified PII with the specified internal organizations?

N/A

Information is shared to allow each Principal Office the capability to ensure assigned users are in compliance with the Department's cybersecurity training program requirement. This aligns with the stated purpose in Question 1.2 above.

External

5.4. Will the PII contained in the system be shared with external entities (e.g. another agency, school district, the public, etc.)? If the answer is **NO**, please skip to Question 6.1.

No

5.5. What PII will be shared and with whom? List programmatic disclosures only.⁴

Note: If you are sharing Social Security Numbers externally, please specify to

⁴ If this information is covered by Privacy Act System of Records Notice (SORN) please list only relevant programmatic disclosures listed under the Routine Uses section.

whom and for what purpose.

N/A

[Click here to enter text.](#)

5.6. What is the purpose for sharing the PII with the specified external entities?

N/A

[Click here to enter text.](#)

5.7. Is the sharing with the external entities authorized?

N/A

[Click here to select.](#)

5.8. Is the system able to provide and retain an account of any disclosures made and make it available upon request?

N/A

[Click here to select.](#)

5.9. How is the PII shared with the external entity (e.g. email, computer match, encrypted line, etc.)?

N/A

[Click here to enter text.](#)

5.10. Is the sharing pursuant to a Computer Matching Agreement (CMA), Memorandum of Understanding (MOU), or other type of approved sharing agreement with another agency?

N/A

[Click here to select.](#)

5.11. Does the project place limitation on re-disclosure?

N/A

[Click here to select.](#)

6. Redress

6.1. What are the procedures that allow individuals to access their own information?

Users have the ability to access their information via the "User Properties" web page within the STLMS application. This page is accessible via:

https://securitytouch.ed.gov/user_properties.k2?accountInfo=1

- 6.2. What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

Users have the ability to correct and update their information via the "User Properties" web page within the STLMS application. This page is accessible via:

https://securitytouch.ed.gov/user_properties.k2?accountInfo=1

Users are not able to manually update their training completion records. For any training completed outside of STLMS, credit is provided by either the OCIO, IAS, Policy and Planning Personnel, or by the STLMS helpdesk, the individual should contact the STLMS helpdesk for further instructions on how to ensure they receive proper credit for any training completed outside of the STLMS site.

- 6.3. How does the project notify individuals about the procedures for correcting their information?

STLMS users are informed on the STLMS homepage that their account username must be identical to their ED Network email address and if they are not certain if they have been assigned an ED Network account and email address, to contact their Contracting Officer's Representative (COR) before registering for a STLMS account. If users currently have an ED Network account and are using a personal or company provided email address to access STLMS, users are advised to contact the STLMS helpdesk. Additionally, users have the ability to contact STLMS support personnel via the email address stated in the Privacy Policy.

7. Safeguards

If you are unsure which safeguards will apply, please consult with your [ISSO](#).

- 7.1. Does the principal office work with their CSO/ISSO to build privacy & security into the system and build privacy extensions to the extent feasible?

Yes

- 7.2. Is an Authority to Operate (ATO) required?

Yes

7.3. Under [NIST FIPS Pub. 199](#), what is the security categorization of the system: **Low, Moderate, or High?**

N/A

Low

7.4. What administrative, technical, and physical safeguards are in place to protect the information?

In accordance with ED's access control policies, STLMS user access is granted based on the need to know and the least privilege required to perform his/her duties. Specific technical privileges are limited to those specifically required for a specific job or an individual's position. Additionally, the firewall provides Intrusion Detection System/Intrusion Prevention System functionality and sends alerts if suspicious traffic to the STLMS is detected and/or blocked. STLMS logs user activities and retains an audit trail at the page level. Failed login attempts are logged along with the IP address and browser information. The audit trail follows users from page to page including user ID and IP address information. The audit logs are accessed by system administrators from within STLMS. STLMS administrators are responsible for configuring and administering the firewall to block unwanted traffic and to protect STLMS from unauthorized access from the Internet. All unauthorized functions, ports, protocols, and/or services are prohibited. Networks and systems are also monitored by an intrusion detection/prevention system that alerts personnel of potential compromises. The intrusion detection/prevention system is constantly monitored and security events evaluated as they occur by the STLMS system administrators.

7.5. Is the information in the system appropriately secured in accordance with the IT security requirements and procedures as required by Federal law and policy?

Yes

7.6. Has a risk assessment been conducted where appropriate security controls to protect against that risk have been identified and implemented?

Yes

7.7. Please describe any monitoring, testing or evaluation conducted on a regular basis to ensure the security controls continue to work properly at safeguarding the PII.

STLMS system performs audit monitoring, analysis and reporting. STLMS administrators conduct internal and external network vulnerability scans at monthly intervals and after any significant change in the network. Testing of the STLMS Contingency Plan is an essential element of a viable contingency capability and is conducted at least annually. This enables plan deficiencies to be identified and addressed prior to implementation during an actual disruption or disaster. Each element of this plan is included in the testing schedule to confirm the accuracy of individual recovery procedures, the effects on Departmental operations and assets, and the overall effectiveness of the plan.

8. Auditing and Accountability

8.1. How does the system owner assess and ensure that the PII is used in accordance with stated practices in this PIA?

A risk assessment is conducted for STLMS system as part of the certification and authorization process. Risk assessment activities include reviewing STLMS documentation, interviewing designated STLMS management and technical personnel, and observing controls where STLMS is physically located. The vulnerabilities identified during the risk assessment of the system will be assigned a risk level of high, medium, or low. This qualitative risk assessment approach enables STLMS management to make informed risk-based business decisions.

System owners/managers are required to update risk assessments at least every three (3) years or whenever there is a significant change to the system, the facilities where the system resides, or other conditions that may impact the security or authorization status of the system as required by OMB A-130. The system owner/manager may acquire a third party to conduct the assessment or use in-house personnel.

8.2. Does the system owner continuously monitor and audit the privacy controls to ensure effective implementation?

Yes

8.3. What are the privacy risks associated with this system and how are those risks mitigated?

Privacy risk are minimized due to the non-sensitive nature of the PII collected, such as would be found on a business card and information on whether mandatory training has been completed. Risks are mitigated by complying with NIST 800-53 Rev. 4 privacy controls in conjunction with the Department of Education privacy and security guidance.