Reset Form PRINT

ILLINOIS DEPARTMENT OF HUMAN SERVICES

SECURITY AND PRIVACY QUESTIONNAIRE

VERSION 4.1 (03/2018)

Prepared By (Disclosure Officer):

Organization/Agency/Entity Name:

Date:

All red questions/responses are **Required** for the SPCQ to be Approved.

The Security and Privacy Questionnaire (SPCQ serves to outline your Organization/Agency's baseline security and privacy controls as they relate to the Data Sharing Agreement (DSA contractual requirements to access the Illinois Department of Human Services (IDHS data, documents and electronic media.

The baseline control questions are in accordance with the Federal and State laws, policies and audit compliance regarding how IDHS provides security and privacy of our client's data and personal information.

The questions are not all inclusive as each IDHS Application or System is different, however, these questions do provide a place from which to develop further discussion and ensure your Organization/Agency meets these security and privacy requirements in regards to IDHS data.

This Questionnaire is an **Annual Requirement of the DSA**. You will be given a copy of the final, approved SPCQ to maintain for your records. Each year, you will complete the form and re-submit for approval.

INSTRUCTIONS

Please answer all of the following questions as they relate to your Organization/ Agency to the best of your knowledge. You may need help from the state program staff and program IT personnel for the required technical information. The DSA may contain some of the information required for input to this form.

If your Organization/Agency is providing a control not listed in a Section, please provide additional information in the space provided. If more space is needed, please attach additional pages with reference to the question you are answering.

The following sections are either in relation to your overall computer/network security or specific information regarding the IDHS system/data for which you are requesting access. Note:

- Please do not leave any question unanswered, unless instructed to skip.
- Please explain in the "Additional Information/Other" text box if you are or are not implementing security as listed in the section.

IF YOUR ORGANIZATION CONTRACTS INFORMATION TECHNOLOGY SERVICES OR SHREDDING SERVICES:

If a Vendor is managing, administering or providing any of the below services, a signed copy of the Nondisclosure/Confidentiality Agreement between your Agency/Organization and the vendor is **required**. This may be included as a confidentiality clause within your vendor contract or in a separate signed document. Either MUST be submitted with the SPCQ.

- **Performs Computer/server/network maintenance;**
- **Provides Data backup, storage, and access to data;**
- **Accesses your computers, servers or computer network equipment;**
- **Provides administrative functions to systems or data / provides your usernames/passwords;**
- **Provides document shredding or storage services;**
- **Cloud Service Provider: Must be FedRAMP Certified. To verify go to https://www.fedramp.gov/.**

If you have questions or concerns in completing this questionnaire, please contact the IDHS program representative or the IDHS Bureau of Information Security, 217-524-2405.

SECTION 1: GENERAL INFORMATION

1.1: CONTACT INFORMATION TABLE

Contact First Name:	Contact Last Name:
Email Address:	Job Function/Title:
Street Address:	
City:	State/Providence:
Zip Code:	Telephone Number:

1.2: ORGANIZATION/AGENCY TYPE (SELECT BELOW OR PROVIDE TYPE IN "OTHER")

State Agency: ○ Provider: ○ Contracted State Organization: ○

Other (Please Specify):

1.3: APPLICATION/SYSTEM ACCESSING (PLEASE SELECT OR IF NOT LISTED, PROVIDE APPLICATION/SYSTEM NAME)

Please select the application/system for which the DSA covers from the drop down below. "Primary" refers to the main or only system listed in the DSA. "Secondary" systems must also be listed in the DSA. Not all DSA's include a Secondary application/system.

Primary Application/System Secondary Application/System (if applicable)

Additional Application/System access or Additional Information:

Reset Page

SECTION 2: IDHS SYSTEM/DATA USE AND ACCESS

This section discusses what IDHS Systems/Data is to be accessed, stored, and destroyed. Please be specific and if necessary, include information in the "Additional Information" section provided.

2.1: PLEASE SELECT THE TYPE(S) OF IDHS SYSTEM/DATA TO BE VIEWED BY YOUR ORGANIZATION.

□ Personally Identifiable Information (PII)

□ Medical Records/Personal Health Information (PHI)

□ Social Security Numbers

□ Federal Tax Information

Other Data Type (please specify): □

2.2: HOW YOUR ORGANIZATION WILL BE INTERACTING WITH IDHS SYSTEMS/DATA (Only one can be selected. Please read each carefully before selecting the appropriate choice)

○ **SEND ORG ONLY:** Upload/send Organizational information only. Once Organization data is uploaded, Organization can no longer access data in the IDHS system/ data source. No IDHS or uploaded Organization data is accessed, viewed, downloaded, printed, or stored.

○ **SEND and RECEIVE ORG ONLY:** Organization's data is sent to IDHS system/data source and only Organization data is received by or accessible to the Organization. No IDHS Data is viewed, accessed, or stored.

○ **READ IDHS ONLY:** Accessing/ Reading IDHS system/data only; No download, printing or storage of IDHS Data or input of Organization's data.

○ **READ and RECIEVE IDHS ONLY:** Accessing/Reading IDHS system/ data and download, print, or store IDHS Data (electronic and/or paper), however no input of Organization's data into the IDHS System.

○ **SEND and RECEIVE BOTH ONLY:** Organization can access IDHS System/Data. Can download, store IDHS Data for use in Organization. Organization can input Organization data into IDHS system/ data source.

Reset Page

2.3: HOW WILL YOUR ORGANIZATION USE AND MAINTAIN IDHS DATA

IDHS Data will be used to:

□ Determine Eligibility in IDHS Program(s).

□ Determine Eligibility in Organization's Program(s).

□ Determine Eligibility in State Program(s) and Organization's Program(s).

□ Match IDHS Data to Organization's data.

□ IDHS Data used to conduct State approved research or study.

□ Organizational reporting purposes only.

□ Other (Please Specify): □

2.4: HOW WILL YOUR ORGANIZATION ACCESS OR TRANSFER INFORMATION TO THE IDHS SYSTEM/DATA SOURCE

□ **Secure Electronic Transfer Method** (select one if applicable):

Tumbleweed: ○ ConnectDirect: ○ Email: ○

Virtual Private Network (VPN): ○ Mainframe Access: ○ Fax: ○

Note: FTI cannot be faxed

State Move-It Process or other Secure File Transfer Protocol (SFTP) Utility: ○ Secure Web Application/Program: ○

□ **Non-Electronic Transfer Method** (select one if applicable):

Postal Mail: ○

□ CD/DVD

□ USB (Flash/Thumb Drive)

□ Hardcopy (Paper)

Hand Delivery: ○

□ CD/DVD

□ USB (Flash/Thumb Drive)

□ Hardcopy (Paper)

Reset Page

2.5: WHAT TYPE OF ACCESS ACCOUNT WILL BE REQUIRED TO ACCESS IDHS SYSTEM/DATA

This information should be available from the IDHS Program Point of Contact assisting with the development of the DSA.

○ RACF/BlueZone (Mainframe Access only)

○ External Illinois.gov (External Organizations/Agencies

○ Public Illinois.gov (general public use)

○ Application specific ID (ID only exists in a specific program or application)

○ Not Applicable:

- Not accessing or viewing IDHS systems/data

2.6: IDHS DATA STORAGE

○ Organization is storing IDHS Data. **Must complete this Section.**

○ Organization is NOT storing IDHS Data (neither paper nor electronic). **Go To Section 3**

2.6.1: If yes, in what form is the data being stored:

□ **Electronic and Paper.** Complete all questions, then proceed to **Section 3**.

□ **Electronic Only** (saved to computer, servers, etc.). Complete **2.6.2 thru 2.6.4**, then proceed to **Section 3**.

□ **Paper (Hardcopy) Only.** Complete **2.6.2, 2.6.3 and 2.6.5**, then proceed to **Section 3**.

2.6.2: IDHS Data (electronic or paper) is stored (select one):

○ Separately

○ Commingled (**If selected, answer the below question**).

□ IDHS data can be separated easily for return/destruction of IDHS data.

Reset Page

2.6.3: **Where is IDHS Data stored** (paper or electronic):

□ On-site at Organization

□ Off-site at:

- □ Organization Data Center/Facility.
- □ Vendor’s Data Center/Facility.
- □ *Cloud Storage: Must be FedRAMP Certified.
  - □ Verification of FedRAMP Certification is included.

2.6.4: Storage of electronic IDHS Data:

□ IDHS electronic data <u>will NOT be backed up</u>. **Go to Section 3**.

□ IDHS electronic data <u>will be backed up regularly</u>. **Complete 2.6.4.1**. questions.

2.6.4.1: IDHS electronic data will be backed up to:

- □ Server
- □ Virtual Machines
- □ Tape/Disk
- □ USB/Thumb Drive
  - □ USB drive is stored in secure location with limited access.
  - □ IDHS PHI/SSN Data is stored on encrypted USB/Thumb Drive.

Additional Information/Other (please specify):

Reset Page

2.6.5: **Storage of IDHS Data on Paper (Hardcopy):**

□ Documents are stored in a secure location with limited access, i.e. locked filing cabinets with limited personnel having key or room access.

□ Disposal of IDHS data on paper is in accordance with DSA.

NOTE: If a shredding service/vendor is to be used for IDHS data destruction, a signed copy of the contract is required to be submitted with the SPCQ. See Page 2 for more information.

SECTION 3: **ORGANIZATION SECURITY, POLICIES AND STANDARDS**

For each subsection, check any/all boxes that describe your Organization security. If none apply, please give us more information in "Additional Information" text box. If additional space is needed, please attach to the SPCQ.

3.1: **ORGANIZATIONAL SECURITY**

□ Organization has a designated, internal Information Technology Department that handles all IT and security related activities.

□ Organization has designated, internal Information Security Department that handles all IT security functions, compliance and auditing.

□ Small organization with Executive/Management oversight on all IT and Office functions. No internal IT department or personnel.

□ Outside IT Vendor handles Organizational's IT and IT Security functions. **NOTE:** Signed contract/confidentiality agreement must be submitted. See Page 2 for more information.

□ Additional Information/Other: □

3.2: **ORGANIZATION SECURITY AND PRIVACY POLICIES**

□ IT security strategy document that details Organization's security vision, mission statement, and Security Management Structure.

□ Written security and privacy policy is published and available to all users, contractors and all concerned parties. Policies include Internet Usage, Acceptable Use and Email Use.

(cont. next page)

Reset Page

□ Additional Information/Other:

If Organization is accessing/viewing IDHS PII/PHI:

□ Organizational Users have/will have undergone a security and privacy awareness-training program and annually thereafter per the DSA.

□ Organizational Users are aware of their personal liability and any potential ramifications if they aid, abet, or participate in a data breach incident involving the organization.

SECTION 4: **ORGANIZATION ACCESS CONTROL**

This section applies to how your Organization/Agency provides access to the Organization's computers/network.

4.1: **ACCESS CONTROL**

□ There is a documented process in place to approve new accounts and modify user privileges.

□ User privileges are based upon job function or assigned roles in the network.

□ User privileges are revoked in a timely basis.

□ User access/privileges are reviewed at least annually.

□ Background checks are conducted for employees/contractors.

□ Additional Information/Other:

4.2: **ORGANIZATION ACCOUNT MANAGEMENT**

Password management is a REQUIREMENT for accessing IDHS data. A username and password MUST be established on all computer/workstations. The account and password must have some standards established in regards to password expiration, length, etc.

□ Organization enforces a password management process:

  □ Unique username and password for user authentication is required.

Reset Page

□ Accounts configured to require password changes after set amount of time, example: every 60 days.

□ Accounts configured to disable or delete after a set amount of time, example: inactivity (haven't logged in) over 90 days.

□ Passwords contain numbers, letters and/or special characters and character length of no less than 8.

□ User identity is verified through a government/student issued Photo ID,

□ Additional Information/Other:

4.3: ORGANIZATION'S ACKNOWLEDGEMENT OF REQUIRED USER DOCUMENTATION AND TRAINING

Each Authorized User of an IDHS system/data must:

□ Sign a Confidentiality Statement.

□ Complete annual Computer Security Awareness Training.

□ Complete annual Health Insurance Portability and Accountability Act (HIPAA) for accessing Protected Health Information. (if applicable).

SECTION 5: ORGANIZATION'S SYSTEM AND NETWORK SECURITY

□ Organization uses a wireless network for accessing/viewing IDHS system/data.

  □ Wireless network is secured/encrypted in accordance with Federal Information Processing Standards (FIPS) 140-2, an example: utilizing WPA/WPA2.

□ Remote accessing of organization's network is only through a Virtual Private Network (VPN).

□ Organization performs patch management on systems/network.

Reset Page

- □ Operating system (Windows/Mac Updates), software and network patches are applied within an acceptable time frames.

□ Virus protection/detection applied on applicable software/equipment.

- □ Virus definition files are up to date.
- □ Email attachments, internet downloads and other potentially malicious extensions (i.e. .exe, .zip, etc.) are pre-screened for viruses.

□ Additional Information/Other: □

SECTION 6: **PHYSICAL SECURITY**

□ Physical security controls such as locked buildings, entry keypads, alarms, cameras or guards are in place.

□ Visitor access is monitored through visitor logs and/or escort.

□ Data Center/Server Room access is limited to specific personnel and secured through door locks, keypads or other barriers for unauthorized entry.

SECTION 7: **SECURITY CONTROL TESTING AND SYSTEM COMPLIANCE**

7.1: **Security assessments are performed to test IT security and privacy controls.**

○ Security assessments are conducted either internally or externally.

○ Security Assessments are NOT performed. (Please provide Additional Information/Other below.)

□ Vulnerability scanners utilized to detect security control weaknesses.

□ High risk vulnerabilities fixed as soon as possible.

□ Additional Information/Other: □

7.2: **System logs are reviewed.**

○ System logs are reviewed regularly.

○ System logs are NOT reviewed. (Please provide Additional Information/Other below)

□ Anomalies or inappropriate use/access is investigated.

□ Additional Information/Other: □

Reset Page

SECTION 8: **SECURITY INCIDENT HANDLING AND REPORTING AND AUDIT COMPLIANCE**

ACKNOWLEGMENT IN REGARDS TO IDHS SYSTEM/DATA

□ Organization/Agency has/will have appropriate procedures in place to report security or privacy incidents (unauthorized disclosure or use involving PII/PHI, or suspected incidents involving IDHS system/data.

□ Organization will promptly report incidents involving IDHS data to Security Contacts listed in the SPCQ immediately or within 24 hours of incident discovery. See DSA for specific information to be reported.

□ Organization acknowledges that IDHS reserves the right to audit our Agency or make other provisions to ensure that the Organization is maintaining adequate safeguards to secure the IDHS information. The Organization understands that audits ensure that the security policies, practices and procedures required by IDHS are in place within the Organization.

□ Organization will maintain records (confidentiality statements, training records, Authorized User lists, etc.) in relation to the Data Sharing Agreement for three (3 years unless otherwise stated in the DSA.

SECTION 9: **IDHS SECURITY AND PRIVACY CONTACTS**

IDHS BUREAU OF INFORMATION SECURITY:

100 South Grand Ave, East

Springfield, IL 62762

217-557-6614 / DoIT.DHS.MISSecurity@illinois.gov

IDHS HIPAA/PRIVACY OFFICER, DEPUTY GENERAL COUNSEL

100 West Randolph, Suite 6-400

Chicago, IL 60601

312-814-3773 / DHS.HIPAA@illinois.gov

Reset Page

SECTION 10: ORGANIZATIONAL SIGNATURES

I acknowledge that I've been presented and reviewed the responses laid out in the Security and Privacy Questionnaire as part of the IDHS Data Sharing Agreement (DSA) contractual requirements. I understand that I must meet the technical, administrative, and physical controls regarding security and privacy for the data/system type and category of data covered in the DSA as required by federal, state, and IDHS statutes, regulations, and policies. I further understand that if there are changes to my IT environment that may affect the security and privacy controls reported herein that they must be reported to the IDHS CISO for evaluation to ensure continued compliancy with the standards and requirements outlined in the DSA.

Disclosure Officer Signature (Individual who completed this form).

Date:

Print Disclosure Officer Name

Organization Executive Officer Signature

Date:

Print Organization Executive Officer Name

Once form is completed and signatures above affixed:

- Save form and attach to email.
- Send email to:
  - **IDHS Program Representative** with whom your Organization is working with in regards to the Data Sharing Agreement
  - **IDHS Bureau of Information Security:** DoIT.DHS.MISSecurity@illinois.gov

Reset Page