Illinois Department of Human Services

Data Sharing Agreement

Security and Privacy Controls Questionnaire

Version 3.5

Prepared By: ____

Organization/Agency (Entity) Name: ______________________________

Date: ____________________

Data Sharing Agreement

Security and Privacy Controls Questionnaire

Instructions

This questionnaire 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 place to start and from which to develop further discussion and ensure your Organization/Agency meets our requirements in securing our data.

Please answer all of the following questions to the best of your knowledge. You may need to get help from IDHS program staff and your IT personnel for some of the more technical information as this should have been discussed with IDHS program staff while working through the DSA process.

For each question, choose an answer of either 'Yes' or 'No'. If 'Yes' is selected, please check all of the additional sub points that apply to your Organization/Agency. Please provide any relevant additional information in the space provided.

Due to the size of your organization or details regarding the type of DSA not all questions may be applicable. If there are any questions that you feel are not applicable to your company, please check 'No' and explain in the 'Additional Information' section at the end of each question.

IF YOU HAVE A CONTRACTED IT VENDOR:

We will need a **copy of the contract** with the IT vendor if they handle any of the following:

- Computer/Server Maintenance
- Data Backup/Access to Data
- Access to your computers, servers or computer network equipment
- Administrative Access to Systems or Data / Provide your usernames/passwords

The Questionnaire MUST signed by the IT Security Officer/Disclosure Officer (who filled out the form) and the Director/Executive from the Organization/Agency.

It is advisable for the Agency to collect and maintain documented supporting evidence to the answers given in this report for auditing purposes and in the event of an IDHS Internal Control On-Site Review.

This Questionnaire will be 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.

If you have questions or concerns in completing this questionnaire, you may contact the IDHS Bureau of Information Security, Chief Information Security Officer at 217-557-6614.

General Information

Contact First Name:	Contact Last Name:
Email Address:	Job Function/Title:
Agency:	
Street Address:	
City:	State/Province:
Zip Code:	
Telephone Number: ( )	

Select your Organization/Agency type from the below. If not listed, please select other and explain:

Contracted State Organization □ Researcher □ State Agency □ Provider □

Other: ______________________________

Describe what your Organization/Agency does:

If text does not fit in window, please attach separate narrative to form with item identified.

What is the Application/System name that you will be accessing?

For what purpose are you using the Application/System?

The following sections will be asking a series of Yes/No and fill-in-the-blank questions regarding various security and privacy technology controls. They are either in relation to your overall computer/network security or specific information regarding the IDHS system and data you are accessing.

Please do not leave any question blank.

If it does not apply to your organization please answer **"No or N/A"** and please explain in **"Additional Information"** or space provided to explain why the control(s) is not applicable or implemented and what your organization does to provide security or privacy in that area.

Security Organization, Policies and Standards

If you are a small Organization/Agency, without a formal IT structure or policies, in the "Additional Information" section, state how you handle computer/IT security in your organization/agency/office.

Some small offices (2-3 staff) may not have formal, written policies. If this is true of your situation, please explain in the "**Additional Information**" section. Having such written policies is a good practice especially for those dealing with Confidential or Sensitive Information as it helps staff know how to handle such information and what to do if something happens unexpected, like losing information or identity theft.

Does your company have an information security infrastructure and organization?

No ○ Yes ○ If Yes, select all below that apply. If No, please explain in "Additional Information:"

□ There is an IT security strategy document that details company's security vision, mission statement, and Security management structure.

□ The board of directors or audit committee provides oversight for the security function.

□ A security officer (CISO or CSO) is designated within or outside the IT organization. Other

□ A Chief Privacy Officer is responsible for management and compliance with your privacy policy.

□ The name and contact information for the security contact has been communicated to users.

Additional information:

If text does not fit in window

Does your company have information security and privacy policies?

No ○ Yes ○ If Yes, select all below that apply. If No, please explain in "Additional Information:"

□ A written information security policy is enforced that includes Internet Usage, Acceptable Use and Email Use

□ Security policies are reviewed at least annually and any changes are approved by the Governance Committee

□ Security and privacy policies are published and made available to all users, contractors and all concerned parties

□ Privacy policy is reviewed and approved by a qualified attorney. Users must reconfirm their acknowledgement of security and privacy policies at least annually.

□ Users have undergone a security and privacy awareness-training program. Employees aware of their personal liability and any potential ramifications if they aid, abet, or participate in a data breach incident involving the organization.

The following areas are addressed in documented security policies:

□ Business Continuity Management
□ Security Assessment and Compliance
□ Electronic Access Control
□ Incident Response
□ Data Protection
□ Password Management
□ Physical Access
□ Remote Access
□ Systems Development & Maintenance
□ Web Application Security

□ Change Control
□ Computer & Network Management
□ Email Usage and Protection Encryption
□ Information Asset Classification
□ Internet Usage
□ Personnel Security and Hiring Standards
□ Privacy & Confidentiality
□ Security Awareness Training
□ Vendor/Third Party Management
□ Virus Protection

Additional Information:

If text does not fit in window, please attach separate narrative to form with item identified.

Are policies and procedures are in place to comply with the necessary Privacy requirements that govern your industry?

No ○ Yes ○ If Yes, select all below that apply. If No, please explain in "Additional Information:"

- □ Privacy policies address the following:
- □ Policies include procedures to prevent the wrongful release, disclosure of Sensitive Data
- □ Define requirements if share data with third parties.
- □ Require contracts with vendors and others with whom you share or store Sensitive Data require the other party to defend and indemnify you for legal liability arising from any release or disclosure of the information due to the negligence of the vendor or other party.
- □ Require all vendors to whom you outsource data processing or hosting functions to demonstrate adequate security of their computer systems.
- □ Vendors must supply SAS70 or CICA Section 5970 Vendor shared assessments (BITS)

Additional information:

If text does not fit in window, please attach separate narrative to form with item identified.

Do your company's policies address access to data based on a data classification scheme?

This means, does your company classify certain information such as Sensitive or Public, and then place restrictions on who can view each type of classified information. For instance, only certain staff can access information marked Confidential.

No ○ Yes ○ If Yes, select all below that apply. If No, please explain in "Additional Information":

- □ Data classification policies are based on risk assessments.
- □ Data protection requirements are defined and documented. Information owners are responsible for the protection of the data they own.

Additional information:

If text does not fit in window, please attach separate narrative to form with item identified.

Does your hiring policy/process require a full background check?

A background check is not a requirement for data sharing with IDHS, however, a screening process is desirable for those personnel who will be accessing IDHS data due to Federal requirements regarding data security and privacy.

No ○ Yes ○ If Yes, select all below that apply. If No, please explain in "Additional Information":

□ All employees

□ All Independent Contractors

□ Others employees:

□ All applicable background checks are done for your organization: Criminal, Educational, Credit, drug and Work History

□ Not Required. If not, please explain why and/or other methods of screening employees:

Additional information:

If text does not fit in window, please attach separate narrative to form with item identified.

Access Control:

The section has to do with how your Organization/Agency provides access to your computers, access to computer files and folders that might have confidential or sensitive information. You may need assistance from your IT Department or whoever assigns/manages your username and passwords for the following information.

Do your company's access control procedures address access to sensitive systems, files and directories?

Meaning, are can everyone access all the files and folders on a computer, drive or network or only specifically authorized personnel based on job duties or position?

No○ Yes ○ If Yes, select all below that apply. If No, please explain in "Additional Information":

□ Procedures for access to mission critical systems and Sensitive Data (e.g. company financial data, customer data, etc.) include user authorization and authentication.

□ Files stored on servers are protected from unauthorized access or use. Access to system files and directories is explicitly restricted to authorized IT personnel.

Additional information:

If text does not fit in window, please attach separate narrative to form with item identified.

Does your company have a process for managing user accounts?

This question refers to whether your Organization/Agency has an established process for when personnel need a computer account on your Organization/Agency's computer and/or network. This may be a formal or informal process. If you answer "No" please explain why. If there is an informal process, then the answer would be "Yes" and you would then explain the process in "Additional Information" section.

No ○ Yes ○ If Yes, select all below that apply. If No, please explain in “Additional Information”:

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

□ User privileges are based upon job function or role-based access. User privileges are changed within one week for internal transfers.

□ User privileges are revoked for terminated users within 2 business days of the termination.

□ Users are required to verify their identity prior to a password reset. User privileges are reviewed at least annually.

Additional information:

If text does not fit in window, please attach separate narrative to form with item identified.

Does your company enforce a password management process?

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

Industry Best Practice Password Standards are: Reset passwords: 30 days / Disabling an account after 60 of days of inactivity / Delete accounts after 90 days of inactivity / Accounts reviewed annually / Minimum of 8 characters in length / 3 login in attempts before lock out / Applications/session termination after 15 minutes of inactivity / At least 3 of the following: uppercase, lowercase, number, special character. **These are recommendations and your standards differ. However, depending on the IDHS data you request to access, IDHS may request certain standards be applied for access to be granted.**

If you answer "No" to the below, you must state that you will be enforcing accounts and passwords or why you are unable to do so. A determination will be made by the State if an exception will be allowed or access be denied.

No ○ Yes ○ If Yes, select all below that apply. If No, please explain in “Additional Information”:

□ Unique username and password for user authentication is required.

□ Password complexity scheme is in place and is technically enforced where feasible or testing is performed to ensure compliance.

□ Technology is configured to require users to change passwords at least every 30 days. Account disabled after 60 days of inactivity.

□ Technology is configured to require privileged users to change passwords at least every 30 days. Passwords cannot be reused for at least 10 changes.

Additional information:

If text does not fit in window, please attach separate narrative to form with item identified.

How do users receive a Username/Password from your Organization/Agency and how is identity verified?

This is in regards to your users accessing your computers and network and how you verify their identity, i.e. driver's license, birth certificate, etc. This is not how users access IDHS applications or programs.

If text does not fit in window, please attach separate narrative to form with item identified.

Please complete the following regarding Password Standards/Rules. Industry Best Practice Password Standards are listed above. **All blanks MUST be completed**:

Expire every_____ days	*Disabled after_____ days inactivity	*Deleted after_____ days inactivity
*Reviewed _______________________________	At least_____ characters in length	Lock after_____ failed attempts
Must contain at least_____of the following: uppercase, lowercase, number, special character		*Application/Session configured to lock/terminate after___minutes of inactivity.

*Not a Password Standard but is an Access Security Control that is must be set.

Do you require your users to complete the following?

Confidentiality Statements and Computer Security Awareness Training are **REQUIRED** as part of the Data Sharing Agreement with IDHS. HIPAA Training is required only for those Organizations/Agencies that will be accessing Medical Records/Protected Health Information.

Sign a Confidentiality Statements that include the safeguards required to protect the data, and the civil and criminal sanctions for noncompliance contained in the applicable federal and state laws, including Section 453(1)(2) of the Social Security Act. 42 U.S.C. § 653(1)(2).	No ○ Yes ○
Take annual Computer Security Awareness Training:	No ○ Yes ○
Take annual HIPAA Training: Per the Privacy Act of 1974, HIPAA Security and Privacy Rules, and other federal and state laws governing computer security	No ○ Yes ○

System Security

The section has to do with how your computer or computer network is secured internally and from the outside (external or remote). You may need assistance from your IT Department or whoever administers or manages your computers or network.

For the purposes of this Questionnaire, a few definitions to help with answering questions or providing Additional Information to explain a No or N/A response:

Computer Network: Typically larger Organization/Agencies. Set of computers or computer systems connected together for the purposes of sharing resources such as files, folders, directories, printers, etc.

Stand-Alone Computer: A computer **not** connected to a network of other computers, systems, **or to the internet. As such, this computer would NOT be able to access a web-based IDHS application or program.**

Computers on a network but not on a centralized server: This is more likely in small offices where a few computers are connected to the Internet through a modem/router but unable to communicate to each other, i.e. do not share files, folders or other network resources (printers). The modem/router should have a firewall built-in.

Are controls in place to secure network access?

No ○ Yes ○ If Yes, select all below that apply. If No, please explain in "Additional Information":

□ There is a documented process in place to activate new network connections.

□ Extranet connections are limited and secured (e.g. via firewall rules established as required by a documented business need).

□ End Point security access is restricted based on machine or user NAC (Network authentication controls) authentication.

Additional information:

If text does not fit in window, please attach separate narrative to form with item identified.

Does your Organization/Agency authorize, monitor and control all methods of remote access to your network?

No ○ Yes ○ If No, please explain in "Additional Information":

Additional information:

If text does not fit in window, please attach separate narrative to form with item identified.

Are connections from laptops, mobile devices, and remote users into the company's network secured?

No ○ Yes ○ If Yes, select all below that apply. If No, please explain in "Additional Information":

□ Advanced authentication controls like two-factor and certificates are in place for remote access.

□ VPN users are required to have personal firewalls and are restricted from accessing

□ Internet using split tunneling

□ Mobile devices like laptops have hard disk encryption enabled.

□ All Wireless devices use superior form of encryption scheme like (WPA or WPA2) and not (WEP or LEAP) which can be easily compromised

Additional information:

If text does not fit in window, please attach separate narrative to form with item identified.

Will Authorized Users access IDHS data or Information System through a Wireless Local Area Network (WLAN)/WiFi?

No ○ Yes ○

If Yes, WLAN/WiFi is FIPS 140-2 compliant: No ○ Yes ○

WLAN/WiFi utilizes guidelines specified in NIST 800-53, Securing Wireless Area Networks: No ○ Yes ○

Are all systems in your Internal, External and DMZ (physical or logical subnetwork containing and exposing the Organization/Agency's external-facing services) environment secured?

By reading the checkboxes below, you will have an idea of what is meant by securing the environment. Your IT Department or administrator should be able to assist you with answering this question.

No ○ Yes ○ If Yes, select all below that apply. If No, please explain in “Additional Information”:

□ Internet accessible systems are tested for new vulnerabilities

□ Application layer Firewalls are used to protect web servers. Firewall(s) are configured to ensure source(s), destination(s) and protocol(s) definitions are tied back to the business need for each rule.

□ Undesirable web and mail content is filtered using **anti-spam products**

□ Critical applications residing within the internal networks (and behind the firewall) are monitored 24 x 7 for security violations.

□ Secured encrypted communications is used for remote administration of all production systems.

□ Periodic scanning conducted for Rogue Wireless Access points on the Network.

Additional information:

If text does not fit in window, please attach separate narrative to form with item identified.

System Maintenance

Your IT Department or computer/network administrators should be able to assist you with answering the below questions.

No ○ Yes ○ **Agency allows only authorized personnel to perform maintenance on the information system.**

No○ Yes ○ **Agency authorizes, monitors, and controls any remotely executed maintenance and diagnotic activities, if employed.**

Does your company enforce a patch Security management process?

Patch Management is a **REQUIREMENT** for accessing IDHS data. For small organization/agencies not on a centralized server and on Windows based computers, the Windows Automatic Updates are typically adequate for your needs. However, free patch management tools are available. IDHS does not endorse or recommend the following specific tools, however, a list of possible tools are located at http://www.windowsecurity.com/software/Patch-Management/ or google: patch management tools.

No ○ Yes○ If Yes, please select all below that apply. If No, please explain in “Additional Information”:

- □ Vulnerabilities and exploits are monitored on a daily basis by Security Operations Center (SOC) or subscription to MSSP
- □ Security patches or workarounds once identified are prioritized based on Impact and Likelihood analysis.
- □ Security patches or workarounds are implemented within the following timeframe of identification: Please Choose:
- □ Patches are tested on non-production systems before they are implemented. Implementation of patches is centralized for all locations.

Please summarize your patch implementation process

If text does not fit in window, please attach separate narrative to form with item identified.

Additional information

If text does not fit in window, please attach separate narrative to form with item identified.

Does your company have a virus protection program in place?

Virus Protection is a **REQUIREMENT** for accessing IDHS data. IDHS does not endorse or recommend the following specific tools, however, a list of possible free tools are located at http://www.windowsecurity.com/software/Patch-Management/ or google: virus protection tools.

No ○ Yes ○ If Yes, please select all below that apply. If No, please explain in “Additional Information”:

□ Virus protection/detection software is installed and enabled on servers, workstations and laptops.

□ Virus definition files are updated from a centralized server for all devices and released within 24 hours

□ Laptops are forced with patch and virus definition updates before establishing a connection to the trusted network.

□ Email attachments, internet downloads and other potentially malicious extensions are pre- screened for viruses at the ingress points

Additional information:

If text does not fit in window, please attach separate narrative to form with item identified.

You MUST complete the below table. Do not leave any blanks. Insert N/A if not applicable and explain in Additional Information above.

	Software	Version
Virus Protection		
Spam/Spyware Protection		
Intrusion Detection		
Firewall		

Security Controls Testing and System Compliance with Security Requirements

Does your company have a program in place to periodically test security controls?

Testing of security controls is a **REQUIREMENT** for accessing IDHS data. IDHS does not endorse or recommend the following specific tools, however, a list of possible free tools are located at http://www.networkworld.com/article/2176429/security/security-6-free-network-vulnerability-scanners.html or google: network vulnerability tools.

No ○ Yes ○ If Yes, please select all below that apply. If No, please explain in “Additional Information”:

□ Security assessments are based on a risk evaluation and are performed at least once a year.

□ Security assessment processes and methodologies are documented. Access to security assessment tools and utilities and the directories where they are stored are restricted to authorized personnel.

Security Assessments include the use of:

□ Outside security specialists to perform penetration testing automated vulnerability scanners

□ Policy compliance checking tools (e.g. eTrust, Bindview) Secure configuration checkers

□ Performance tools Modem Wireless Sweeps

□ Source code comparison tools.

□ Security policies and controls are subject to independent reviews and audits.

□ All high risk vulnerabilities are remediated within one month. There is no significant deficiency in audit findings longer than six months.

Additional information:

If text does not fit in window, please attach separate narrative to form with item identified.

Are system logs reviewed for security related events?

Review of system/security logs is a **REQUIREMENT** for accessing IDHS data. For small Organizations/Agencies with limited computers not connected to a central server, go to https://technet.microsoft.com/en-us/library/cc731826(v=ws.11).aspx for more information on how to review security logs on Windows based computers.

No ○ Yes ○ If Yes, please select all below that apply. If No, please explain in “Additional Information”:

□ System log reviews:

□ Occur at least daily

□ Perimeter Logs are correlated to reduce false positives

□ Access Control Logs are consolidated in central location to detect new anomalies and violations

□ Data Leakage is addressed by proactive keyword monitoring on Peripherals (USB) and email attachements.

Additional information:

If text does not fit in window, please attach separate narrative to form with item identified.

Physical Security

This section is concerned with the actual Physical Security of your Organization/Agency. This is especially important for those Organizations/Agencies that will be storing IDHS Data in either paper or electronic (computer files, DVD, tapes, servers, USB/Flash drives). It is still important for those simply accessing IDHS Data on their computer in that there is still the possibility of unauthorized personnel viewing such data on personnel's monitors and such.

Some Organization stores IDHS Data (electronic or paper) on-site at their Organization/Agency location while others may store off-site at a Central Data Center or Facility. In instances where IDHS is stored off-site, we need to know the Physical Security of **both** the Organization/Agency and the Central Data Center or Facility housing the IDHS Data. **NOTE: If Cloud services are to be used for IDHS Data, you MUST contact IDHS CISO for additional guidance and requirements.**

Does your company have physical security controls in place?

No ○ Yes ○ If Yes, select all below that apply. If No, please explain in "Additional Information":

□ A security perimeter has been identified and documented, which includes computer rooms, media storage rooms, data centers, etc.

□ Biometric access controls are used to access company data center(s). ID badges are required for employee, visitor and vendor access.

□ Surveillance cameras and guards are in place to monitor premises. Data Center access logs are monitored periodically

□ Smart cards are used for physical and logical security. Physical security management is centralized for all locations

□ Computer, media storage and telecom room access is secured and restricted to authorized personnel.

□ Cables and network ports are protected from unauthorized access. Disposal of computer systems and media storage devices (hard drives, tapes, floppies, CDs, etc) is handled in a secure fashion (i.e. de- magnetization and multiple wipes).

□ Physical security management is centralized for all locations

Additional Information:

If text does not fit in window, please attach separate narrative to form with item identified.

Are keypads used for entry to your building?

No ○ Yes ○ If Yes, is each attempt logged? No ○ Yes ○

If yes, who reviews the access logs? (Name and title):

If text does not fit in window, please attach separate narrative to form with item identified.

Are building/room alarm systems utilized? Please include Name and Title: (e.g. Intrusion Alarms, Security Cameras, Motion Detectors, Exit Alarms)

If text does not fit in window, please attach separate narrative to form with item identified.

For each facility, do visitors/vendors sign a visitor access log?

No○ Yes○

If yes, what information is captured on the log?

If text does not fit in window, please attach separate narrative to form with item identified.

Where is the log stored and for how long?

If text does not fit in window, please attach separate narrative to form with item identified.

Who has access to your Data Center/Server Room (where you keep your servers, routers, and other network equipment) after core business hours? Please include Name and Title.

If text does not fit in window, please attach separate narrative to form with item identified.

How is security enforced after core business hours? For example, 24-hour guards, security camera's, locked building, etc.)

If text does not fit in window, please attach separate narrative to form with item identified.

Data Use and Access

This section discusses what IDHS Data you will be accessing, how you will access the data, whether you will store the data and the security controls regarding its storage. Please be specific and if necessary, include information in the "Additional Information" section provided. You may attach additional sheets if necessary. Answers to these questions will refer back to the Data Sharing Agreement (DSA) that you are entering into with IDHS and you will be held by the requirements in the DSA in regards to the purpose, use, storage and disposal of IDHS Data as outlined in the DSA.

What Type of IDHS Data will you be accessing in the Application/System identified in the General Overview section of this document?

Personally Identifiable Information (PII): □

Social Security Numbers (SSN): □

Medical Records/Personal Health Information (PHI): □

Federal Tax Information (FTI): □

Other: If text does not fit in window, please attach separate narrative to form with item identified.

NOTE: The above information is considered Confidential or Sensitive information which must be protected. PHI, SSN and FTI require extra security precautions such as **ENCRYPTION**.

Encryption is a **REQUIREMENT** for IDHS Data that includes (but not limited to) Social Security Numbers and Protected Health Information.

A list of FIPS 140-1/140-2 Cryptographich (encryption) modules is available at: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm. The hardware or software manufacturer should also be able to tell you if their product is FIPS certified.

Does your Organization/Agency encrypt confidential or sensitive information such as Social Security Numbers, Medical Records/Protected Health Information?

No ○ Yes ○ If yes, please select all below that apply:

□ Public/private keys are used for the encryption of sensitive information. 128-bit encryption products (i.e. TSL, RSA) and/or algorithms (e.g. AES) are used. (IAW FIPS 140-1/NIST)

□ Database encryption is used for sensitive information (e.g. credit card numbers, social security numbers, etc.).

□ Passwords are encrypted.

□ File encryption is used for locally stored materials (e.g. on laptops, etc.)

Additional information:

If text does not fit in window, please attach separate narrative to form with item identified.

When you access the IDHS Application/System, what is the purpose?:

○ **READ ONLY:** Access Application/System to read/view IDHS Data only.

○ **SEND:** Access Application to enter/upload data into the IDHS Application/System.

○ **RECEIVE**: Access Application/System to download and store IDHS Data at your Organization/Agency or Organization/Agency Data Center or Facility.

○ **SEND and RECEIVE:** Access Application/System to send and receive IDHS Data.

How will you use IDHS Data?

□ Use IDHS Data to **determine eligibility**

□ In an IDHS program □ In our Organization/Agency program

□ Create **Paper Documents** (i.e. reports, case files, letters, etc.)

□ Use IDHS Data to **Match data** in our Organization/Agency

□ Use IDHS Data to **conduct a Research or Study**

□ **Distribute or store** IDHS Data □ Paper

□ Electronic Media (i.e. hard drive, server, USB, etc.)

How will you Access IDHS Data:
You may need to contact IDHS program personnel for this information if you do not know how you will access, send or receive IDHS Data.

Tumbleweed connection: □ ConnectDirect: □ Mainframe Access: □

Virtual Private Network (VPN): □ Postal Mail: □ CD/DVD: □

Secure Web Application: □ Email: □ Secure File Transfer Protocol (SFTP): □

Other: If text does not fit in window, please attach separate narrative to form with item identified.

Is IDHS data to be transmitted via fax machine?
Please be aware that Social Security Numbers are considered Confidential and therefore should not be sent through a fax machine unless absolutely necessary. If possible, please redact (i.e. send only the last 4 digits).

Protected Health Information (PHI) if faxed must be handled very carefully. Please contact the IDHS Privacy Officer for more information regarding faxing PHI if applicable. Please ensure a cover sheet is utilized and the fax number is verified to be correct. Documents with Personally Identifiable Information (PII) and PHI must not be left unattended on a fax machine. Fax machines sending such information should be in non-public areas and secured. If you have questions, please contact the IDHS Privacy and Security Contacts listed below for more information on faxing Confidential Information.

NOTE: Federal Tax Information is NEVER to be sent by fax.

No ○ Yes ○ If Yes, where is the receiving fax machine located?

Are all individuals in the receiving location authorized to access IDHS data?

No ○ Yes ○

If No, how is Access limited to only those users authorized to access IDHS Data?

If text does not fit in window, please attach separate narrative to form with item identified.

How will those who are authorized access IDHS Data:
Contact IDHS program personnel for questions regarding what user account type and source will be required for the IDHS Application/System in which you will be accessing.

IDHS provided Username/Password (select account type):

○ Internal Illinois.gov (State of Illinois personnel)

○ External llinois.gov (external entities, Organizations/Agencies)

○ Public Illinois.gov (general public use)

○ RACF/Bluezone (for mainframe access)

○ Application ID (specify): (application specific user account used only by that application or program)

○ Not Applicable, Specify: If text does not fit in window, please attach separate narrative to form with item identified.

Data Storage and Backup

Will your Organization/Agency Store IDHS Data?

No ○ Yes ○ If Yes, select all below that apply. If No, please answer "N/A" for the remaining questions in this section.

□ Data is stored on-site at the Agency.

□ Data is stored off-site at a Data Center/Facility. If at a vendor facility, IDHS must have a copy of the contract to ensure appropriate security and privacy requirements are met.

□ Data is stored in the Cloud

In order for IDHS data to be stored in a Cloud, the Cloud must be FedRAMP Certified, https://www.fedramp.gov/. Otherwise, alternate storage solution for IDHS Data must be determined prior to approval of SPCQ/DSA.

If storing IDHS Data, will it be stored (select one):

Separately ○ Commingled ○

Can IDHS Paper Documents or Electronic Data be located and separated easily?

No ○ Yes ○

Does your Organization/Agency have Backup and Recovery procedures for the Electronic IDHS Data your store?

No ○ Yes ○ If Yes, select answer the below. If No, please explain in "Additional Information":

What is the Backup schedule for the IDHS Data that is stored at the Agency?

Who backs up the information, please include Name and Title?

What type of media is used for the backup (i.e. virtual machine, server, etc)?

What is the retention period of back-up media/ how many generations exist at a time?

Additional information:

If text does not fit in window, please attach separate narrative to form with item identified.

Explain the security and privacy safeguards regarding how Paper Documents and/or Electronic Media containing IDHS data and the devices through which IDHS data is received, stored, processed, or transmitted locked or otherwise secured? Please describe how they are locked or secured, including key control procedures, and/or combination lock control procedures (e.g., restricted access server room, locked server rack, restricted access media library, file room, office, locked cabinets, etc.). If you do not store IDHS Data either paper or electronic, input "N/A"

If text does not fit in window, please attach separate narrative to form with item identified.

Security Incident Handling and Reporting

Incident Handling and Reporting is a **REQUIREMENT** of the Data Sharing Agreement. Organization/Agencies must check the Yes boxes below indicating that you have or will have such procedures in place and will report in accordance with the DSA any security incidents. If these boxes are not checked yes, the SPCQ will not be approved.

□ Our Organization/Agency have appropriate procedures in place to report security or privacy incidents (unauthorized disclosure or use involving PII/PHI), or suspected incidents involving IDHS information.

□ Our Organization/Agency tracks and documents application security incidents on an ongoing basis

□ Our Organization/Agency promptly report incidents involving IDHS data to Security Contacts listed in the SPCQ immediately or within 24 hours of incident discovery

Audit and Accountability

Auditing and Accountability is a **REQUIREMENT** of the Data Sharing Agreement. Organization/Agencies must check the Yes boxes below indicating that you have or will have such procedures in places. If these boxes are not checked yes, the SPCQ will not be approved.

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

□ Our Organization/Agency maintains records (Confidentiality Statement, training records, authorized user lists, etc.) in relation to the Data Sharing Agreement for three (3) years.

Topology

This is not required; however, it may be requested by IDHS if there is a concern regarding the security or privacy controls required for secure transmission or storage of IDHS Data.

Topology diagram(s) is included to show connected, interfaces, protocols, etc.

No ○ Yes ○ If Yes, Please attach.

IDHS Security and Privacy Contacts

IDHS Chief Information Security Officer:
Department of Innovation and Technology, Office of Management of Information Services
Bureau of Information Security and Audit Compliance
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

NOTE: Electronic Signature is not accepted at this time. Please sign in blue/black ink.

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, policies. I further understand that if there are changes to my IT enviroment 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 Date

Print Disclosure Officer Name

Agency Executive Signature Date

Print Agency Executive Name