Intergovernmental Agency / Data Sharing Agreement

Security and Privacy Controls Questionnaire

Version 1.5

Prepared By:

[Insert Agency]

[Insert Agency Address]

[Insert Date]

Intergovernmental Agency / Data Sharing Agreement

Security and Privacy Controls Questionnaire

Instructions

The following questions serve to outline the requesting Agency's baseline security and privacy controls as they relate to the Intergovernmental/ Data Agreement contractual requirements regarding the Illinois Department of Human Services (IDHS) data, documents and electronic media. The baseline control questions are in accordance with (IAW) the National Institute of Standards and Technology (NIST) 800-53r, regarding security and privacy controls. The questions are not all inclusive as each system is different, however, these questions do provide initial baseline from which to develop further discussion and development of an appropriate security plan.

Please answer all of the following questions to the best of your knowledge. You may need to refer certain sections of this questionnaire to other managers in your company for completion. For your convenience, next to each section heading we have noted the job function(s) that may be best equipped to answer the questions within that section

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 company. Please provide any relevant additional information in the space provided.

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 a topic in any section pertains to a service that is outsourced, please answer the questions to the best of your knowledge and/or fill out the additional information section of the question. Please also enter details on the outsourcer that you use in the vendor management section of this questionnaire.

Upon completion, the form must be printed out and signed by the IT Security Officer/Disclosure Officer and the Director from the 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.

General Information

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

Select Agency Type:

Contracted State Organization ☐ State Agency ☐ Provider ☐

Other:

Description of Operations:

System Overview

System Name and Identifier:		
Security Categorization: FIPS 199 Impact Level		
System (based on high water mark of security objectives impact level)	Low Med Select High	
Below is based on high water mark of information type impact level		
Confidentiality: A loss of *confidentiality* is the unauthorized disclosure of information.	Low Med Select High	**Low: Limited adverse effect** on organizational operations, organizational assets, or individuals **Medium: Serious adverse effect** on organizational operations, organizational assets, or individuals.
Integrity: A loss of *integrity* is the unauthorized modification or destruction of information.	Low Med Select	

	High	**High: Severe or catastrophic adverse effect** on organizational operations, organizational assets, or individuals.
Availability: A loss of *availability* is the disruption of access to or use of information or an information system.	Low Med Select High	
General System Description/Purpose:		

List of Connected Systems		
System Name	**FIPPS Category**	**Accreditation Date**

Security Organization

Does your company have an information security infrastructure and organization?

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

☐ 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. Other _____

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

Additional information:

_____

_____

_____

Security Policy and Standards

Does your hiring process require a full background check?

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

☐ All employees Some Employees

☐ All Independent Contractors Others

☐ Not Required, Why?

_____

_____

_____

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

Additional Information:

_____

_____

_____

Does your company have information security and privacy policies?

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

☐ 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
- ☐ Change Control
- ☐ Security Assessment and Compliance Computer & Network Management Electronic Access Control

- ☐ Email Usage and Protection Encryption
- ☐ Incident Response
- ☐ Information Asset Classification and Data Protection Internet Usage
- ☐ Password Management
- ☐ Personnel Security and Hiring Standards Physical Access
- ☐ Privacy & Confidentiality Remote Access
- ☐ Security Awareness
- ☐ Systems Development & Maintenance Vendor/Third Party Management Web Application Security
- ☐ Virus Protection

Additional Information:

_____

_____

_____

Data Type

Type of Data includes the following:

Personally Identifiable Information: ☐ Social Security Numbers: ☐

Federal Tax Information: ☐ Medical Records or other PHI: ☐

Other:

Based on the above, the overall System/Data Categorization is (select one):

☐ Low ☐ Med ☐ High

Access Control:

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

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

- ☐ 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:

_____

_____

_____

Does your company enforce a password management process?

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

☐ 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:

_____

_____

_____

Are controls in place to secure network access?

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

☐ 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:

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

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

- ☐ Advanced authentication controls like two-factor and certificates are in place for remote access.
- ☐ VPN users are require 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:

Does your company have a process for managing user accounts?

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

- ☐ 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:

Is encryption used to protect sensitive information when it is transmitted over external networks?

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:

_____

_____

_____

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

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

☐ 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:

_____

_____

_____

Restrictions

How is Access limited to authorized users:

_____

_____

The Agency restricts access to, and disclosure of, IDHS Data and information system(s) to only Authorized users who require IDHS information to perform their official duties in connection with the authorized purposes specified in the agreement.

Authorized users are prohibited from accessing IDHS information remotely (e.g., telecommuting) and using personally owned devices (e.g. personal computers, mobile/cell phones, MP3 players, USB/Flash drives, etc) or other non-agency furnished equipment used to connect to IDHS information regardless of connection type (e.g., wireless, VPN, Ethernet).

Authorized uses are prohibited from copying or storing IDHS data to mobile media, i.e. laptops, CD/DVDs, USB/Flash Drives, etc.

Authorized users:

Sign a Non-Disclosure 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). ☐

Take annual Computer Security Awareness Training: ☐

Take annual HIPAA Training Per the Privacy Act of 1974, HIPAA Security and Privacy Rules, and other federal and state laws governing computer security: ☐

Authorized users will access IDHS Data:

☐ Using IDHS provided Username/Password (select account type):

Illinois.gov (Internal)
Illinois.gov (External)
RACF/Bluezone
Application (specify): _____

☐ Using Agency provided Username/Password:

How do users receive a Username/Password from the agency and identity verified?

_____

_____

Please complete the below regarding Passwords:

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.

Agency authorizes monitors and controls all methods of remote access: No ☐ Yes ☐

Will Authorized Users access IDHS data or Information System through a Wireless Area Network (WAN)?

No ☐ Yes ☐

If Yes, WAN is FIPS 140-2 compliant:

WAN utilizes guidelines specified in NIST 800-53, Securing Wireless Area Networks: No ☐ Yes ☐

Data Transmission

Data will be (check all that apply):

Sent ☐ Received ☐ Processed ☐ Stored ☐

How is Data to be sent/received:

Tumbleweed: ☐ ConnectDirect: ☐ Virtual Private Network (VPN): ☐ Secure File Transfer Protocol (SFTP): ☐

Secure Web Access: ☐ Mainframe Access: ☐ Postal Mail: ☐

Email: ☐ CD/DVD: ☐

Other:

Encryption: Data is transmitted in a mutually approved and secured data transfer that utilizes FIPS 140-2 compliant; NIST-certified encryption solution: Yes

Is IDHS data to be transmitted via fax machine? No ☐ Yes ☐

Where is the receiving fax machine located?

Are all individuals in the receiving location authorized to access IDES data? No ☐ Yes ☐

Data Use and Access

Data/Information System to be used:

Process to determine eligibility of program ☐	Process to conduct research/study ☐
Create paper documents (i.e. reports, letters, etc.) ☐	Create distributed electronic media (i.e. CD/DVD, Flash Drive, etc.) ☐
Store data ☐	Match data ☐

Data Storage and Backup

Data will ☐ will not ☐ be stored on-site at the Agency.

If stored at Agency, will it be stored (select one):

Separately ☐ Commingled ☐

Can IDHS Paper Documents or data be located and separated easily?

No ☐ Yes ☐

If stored at the Agency, what safeguards are currently in place or will be in place to secure IDHS Data?

What are the Backup and Recovery procedures and schedule for the IDHS Data that is stored at the Agency?

Who backs up the information and on what type of media (i.e. virtual machine, server, etc)?

If Paper Documents or Electronic Media (CD/DVDs, Flash Drives), where are they stored before and after processing?

For Electronic Media, does the Agency keep back-up files? No ☐ Yes ☐

How are files backed up?_____

By whom?_____

On why type of media?_____

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

Physical Security

Does your company have physical security controls in place?

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

- ☐ 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 keypads are used, is each attempt logged?

No ◯ Yes ◯

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

_____

_____

Who monitors any alarm systems? (e.g. Intrusion Alarms, Security Cameras, Motion Detectors, Exit Alarms) (Name and title):

_____

All Paper Documents or Electronic Media containing IDHS data and devices, through which IDHS data is received, stored, processed, or transmitted at these facilities locked or otherwise secured? (e.g., restricted access server room, locked server rack, restricted access media library):

If yes, please describe how they are locked or secured, including key control procedures, and/or combination lock control procedures for each separate facility.

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

If yes, what information is captured on the log? Where is the log stored and for how long?

Who has access to the Data Center/Server Room at the requesting Agency's Headquarters and any State Agency or Contractor contracted with by the requesting Agency after core business hours? (Name and Title)

How is security enforced after core business hours?

Security Incident Handling and Reporting

The Users have appropriate procedures in place to report security or privacy incidents (unauthorized disclosure or use involving PII/PHI), or suspected incidents involving DHS information. No ☐ Yes ☐

Agency tracks and documents application security incidents on an ongoing basis: No ☐ Yes ☐

Agency promptly report incidents involving IDHS data to the Bureau of Information Security and Audit Compliance immediately or within 24 hours of incident discovery: No ☐ Yes ☐

System Maintenance

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

Agency authorizes, monitors, and controls any remotely executed maintenance and diagnostic activities, if employed.

System Security

Does your company enforce a patch Security management process?

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

- ☐ 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:

_____

_____

_____

Additional information:

_____

_____

_____

Does your company have a virus protection program in place?

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

- ☐ 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:

	Software	Version
Virus Protection		
Spam/Spyware Protection		
Intrusion Detection		
Firewall		

Are all systems in your Internal, External and DMZ environment secured?

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

☐ Internet accessible systems are tested for new vulnerabilities and 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:

Compliance

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

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

☐ 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:

_____

_____

_____

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

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

☐ 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:

_____

_____

_____

Are system logs reviewed for security related events?

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

☐ 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 attachments.

Additional information:

_____

_____

_____

Audit and Accountability

IDHS reserves the right to audit the Agency or make other provisions to ensure that the Agency is maintaining adequate safeguards to secure the IDHS information. Audits ensure that the security policies, practices and procedures required by IDHS are in place within the Users.

Agency maintains records (Non-Disclosure Statement, training records, authorized user lists, etc.) in relation to the Data Sharing Agreement for three (3) years. No ☐ Yes ☐

Topology

Topology diagram(s) is included to show connected, interfaces, protocols, etc. No ☐ Yes ☐

IDHS Security and Privacy Contacts

IDHS HIPAA Privacy Officer
Patricia Brown
Deputy General Counsel
100 West Randolph, Suite 6-400
Chicago, IL 60601
312-814-3773
Patricia.M.Brown@illinois.gov

IDHS Chief Information Security Officer:
Kate Atteberry
Department of Management of Information Systems
Bureau of Information Security and Audit Compliance
100 South Grand Ave, East
Springfield, IL 62762
217-557-6614
Kate.Atteberry@illinois.gov

I acknowledge that I've been presented and reviewed the responses laid out in the Security and Privacy Questionnaire as part of the IDHS Intergovernmental/Data Sharing Agreement (IGA/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 IGA/DSA as required by federal, state, and IDHS statutes, regulations, policies.

Disclosure Officer	Date
Agency Executive	Date