SHARED DATA AGREEMENTS

Internal Controls Questionnaire

Version 1.0

Prepared By:
[Insert Agency]
[Insert Agency Address]

[Insert Date]

INSTRUCTIONS

The following questions serve as the Internal Control Questionnaire for the requesting Agency's security procedures relating to the Illinois Department of Employment Security (IDES) documents and electronic media as part of the Shared Data Agreement contractual requirements.

When answering the questions in this document, the answers should be entered on the line directly below the question.

After completion, the form should be printed out and signed by the Disclosure Officer and the Director from the Agency.

The Agency should complete the contact information below for all parties that involved in supplying information.

Name	Title	E-mail

It is advisable for the agency to collect and maintain documented evidence to back to answers to this report in the instance of an audit. Having this evidence on hand will also aid the IDES Internal Controls on-site review.

A. General Information

1. Do you currently possess any IDES data?

    a. If yes, please describe the type of data and what format the data is in? (paper documents, electronic media, etc.)

2. How is data received from IDES? (Tumbleweed, ConnectDirect, other Secure Data Transmission (SDT)-list)

3. Are paper documents or electronic media created from the IDES data (letters, reports, etc.)? If yes, please describe what paper documents or electronic media are created.

4. How are the paper documents or electronic media distributed?

5. Are any paper documents or electronic media provided to a contracted State Agency or Contractor? (e.g., consolidated storage center, offsite storage location)

    a. If yes, please provide the Site Name and Address for each facility that house IDES paper documents or electronic media.

6. What safeguard controls are in place when transmitting and processing the IDES paper documents or electronic media at these locations?

7. Where are IDES paper documents or electronic media stored before and after processing at these locations? (Agency, Data Center, Other-list)

8. For IDES electronic media, do you keep back-up files? If so, how are data files backed up, by whom, and on what type of media?

9. For IDES electronic media, what is the retention period of back-up media and how many generations of back-up files exist at this time?

B. Security

I. Physical Security

10. Please describe the physical security of the requesting Agency's Headquarters and any State Agency or Contractor contracted with by the Agency? (e.g. keypad locked doors, alarm systems, guard desks, locations, hours, etc.)

    a. If keypads are used, is each attempt logged? Who reviews the access logs? (Name and title)

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

11. Are all paper documents or electronic media containing IDES data and devices through which IDES 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)?

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

12. Is IDES data transmitted via fax machine?

    a. Where is the receiving fax machine located? (location in office)

    b. Are all individuals in the receiving location authorized to access IDES data?

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

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

14. Who has access to the Data Center 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)

    a. How is security enforced after core business hours?

II. Application Security

Agencies should supply information in "Section II. Application Security" ONLY if they store or process IDES electronic media in Agency applications.

15. Are application users supplied with unique user IDs?

    a. How does the user receive their user ID?

    b. Are accounts configured to lock after 3 failed login attempts?

    c. Are user IDs disabled after 90 days of inactivity?

16. Is the application configured to lock/terminate the session after 15 minutes of inactivity?

17. Does the Agency track and document application security incidents on an ongoing basis?

    a. Does the Agency promptly report incidents involving IDES data to IDES?

18. Is IDES data transmitted via email?

    a. How is the data protected? (encryption - describe)

19. Does the agency have web-based applications?

    a. Is IDES data accessible through a web site?

20. What software and version is used for Virus Protection?

21. What software and version is used for Spam/Spyware Protection?

22. What software and version is used for Intrusion Detection?

23. Does the Agency provide annual security awareness training regarding the handling of confidential data? If yes, please describe.

    a. Are there records maintained to track employee completion of this training?

Restricting Access

24. Is IDES electronic media kept separate or is it commingled with other information?

25. Can IDES paper documents or electronic media within agency records be located and separated easily?

26. How is access limited to authorized personnel?

Disposal

27. Is paper waste material with IDES data generated?

b. How is the paper waste material destroyed? (recycle bins, locked containers, waste baskets, other container)

c. Is a contractor used to pick up the paper waste material?

i. If yes, please provide the name of contractor:

ii. Where does the contractor take the paper waste material for destruction?

I acknowledge that I've been presented and reviewed the responses laid out here in the Internal Controls Questionnaire as apart of the IDES Shared Data Agreement contractual requirements.

/s/

_____ _____

Disclosure Officer Date

/s/

_____ _____

Agency Executive Date