

# SHARED DATA AGREEMENTS

## Internal Controls Questionnaire

Version 1.0

Effective Date: August 19, 2014

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

[Insert Date]



## Record Keeping Requirements

1. Do you currently possess any IDES data?

a. If so, please complete the following questions for each expired and current executed SDA:

SDA Contract Number:

SDA date of execution:

SDA date of expiration:

Name of Contractor:

Address of Contractor:

Contact Person for Contractor:

Name of Subcontractor 1:

Address of Subcontractor:

Contact Person for Subcontractor:

(Add additional sub-contractors, as needed)

Transmitted Data: Year/Quarters

Transmitted Data: Fields

Do you have data currently stored? (yes/no)

i. If yes,

Address storage location 1:

Address storage location 2:

Address storage location 3:

Address storage location 4:

ii. If no,

Date for data disposal:

Method for data disposal:

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

3. Are data receipts logged?

a. What data elements are captured in the log?

4. Are products/documents created from the data (letters, reports, etc.)? Describe what products/documents are created.
  - a. How are these products/documents tracked and stored until destruction?
5. Upon receipt of data from IDES, how and where is the data electronically distributed?
6. What type of data is received from IDES?
7. Are back-up files stored off-site?
  - a. Where (Site Name and address) are files stored?
  - b. What protections are in place?
  - c. Who currently has access (name & title)?
8. Is electronic media provided to a contracted State Agency or Contractor? (e.g., consolidated storage center, offsite storage location)
  - a. List
  - b. What safeguard controls are in place when transmitting and processing the electronic media at this site?
9. Where is electronic media stored before and after processing? (Agency, Data Center, Other-list)

10. How are data files backed up, by whom, and on what type of media?

11. What is the retention period of back-up media and how many generations of back-up files exist at this time?

## **Secure Storage**

12. Please describe the physical security of the Agency Headquarter? (e.g. keypad locked doors, guard desks, locations, hours, etc.)

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

13. What alarm systems are currently running at Agency Headquarters? (e.g. Intrusion Alarms, Motion Detectors, Exit Alarms)

- a. Who monitors these alarms? (Name and title)

14. Are security cameras used at the Agency Headquarters?

- a. Who monitors the security feed? (Name and title)

15. Please describe the physical security of the Data Center? (e.g. keypad locked doors, guard desks, locations, hours, etc.)

- a. If keypads are used, is each attempt logged?

b. Who reviews the access attempt logs? (Name and title)

16. What alarm systems are currently running at Data Center? (e.g. Intrusion Alarms, Motion Detectors, Exit Alarms)

a. Who monitors these alarms? (Name and title)

17. Are security cameras used at the Data Center?

a. Who monitors the security feed? (Name and title)

18. Are records maintained on the issuance of keys/key cards?

a. How are records maintained? (automated file, written log, etc.)

b. Who is responsible for the issuance of keys/key cards (Name and title)

c. Are periodic reviews conducted to reconcile records and determine if users still need access?

i. Date of last review.

19. Are all electronic media containing IDES data and devices through which IDES data is received, stored, processed, or transmitted locked or otherwise secured, (e.g., restricted access server room, locked server rack, restricted access media library)? If so describe how they are locked or secured, including key control procedures.

- a. Where is the key kept?
- b. Who has access to the key?
- c. How many keys are in existence?
- d. Who maintains the backup keys?

20. Is IDES data locked in a storage cabinet?

- a. Where is the key kept?
- b. Who has access to the key?
- c. How many keys are in existence?
- d. Who maintains the backup keys?

21. Are combination locks used?

- a. How often is the combination changed?
- b. Who controls the combinations?

22. Are ID cards required to be worn by employees at all times?

a. How are ID cards inventoried or managed?

23. Do visitors/vendors sign a visitor access log?

a. What data elements are captured in the log?

b. Who reviews the visitor access log periodically?

24. IRS Publication 1075 recommends a Minimum Protection Standard of two barriers to protect data. Please describe the one that applies to your agency:

- i. Secured perimeter / locked container
- ii. Locked perimeter / secured interior
- iii. Locked perimeter / secured container
- iv. Other (describe)

25. Who has access to the Agency Headquarters after core business hours?

a. How is security enforced after core business hours?

26. Who has access to the Data Center after core business hours?

a. How is security enforced after core business hours?

27. Are files stored at an off-site storage facility?

28. Is this a state-run facility or a contractor site?

a. How is access limited from non-agency personnel?

29. How are the files shipped / transferred to the off-site storage facility?

### **Restricting Access**

30. What identifying information is used to retrieve IDES data?

31. Is IDES data kept separate or is it commingled with other information?

32. Can IDES data within agency records be located and separated easily?

33. After independent verification occurs, what specific data is entered into the system?

34. How is access limited to authorized personnel?

35. Is IDES data made available to personnel outside of agency personnel (contractors, other agencies, etc.)?

a. List personnel/offices and provide a justification.

36. Does the agency have web-based applications?

a. Is IDES data accessible through a web site?

37. Are access log reports monitored to detect unauthorized browsing?

38. Is IDES data transmitted via email?

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

39. 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?

## **Disposal**

40. Is paper waste material with IDES data generated?

- a. Where is paper waste material placed? (recycle bins, locked containers, waste baskets, other container)
- b. How is the paper waste material destroyed?
- c. Who performs the destruction of paper waste material? (Agency Staff, Contractor – list)
- d. Is a contractor used to pick up the waste material?
  - i. Name of contractor:
  - ii. Where does the contractor take the waste material for destruction?

iii. Does agency staff accompany material and view destruction?

41. Is IDES data stored on electronic media (tapes)?

a. How is the data erased? (Degaussed, Written over with 0 (zero) and 1 (one), Written over with new data)

### **Computer System Security**

42. Are there user accounts for the application containing IDES data?

a. How are these accounts managed?

b. Who manages the accounts?

c. Are accounts given the appropriate level of permissions that do not exceed a person's need for their job functions?

d. How often and by whom are accounts reviewed for access need?

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

43. Are application users supplied with unique user IDs?

a. How does the user receive their network user ID?

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

c. Are user IDs archived?

44. Are application passwords set to be a minimum of 8 characters in length?

a. What complexity requirements are tied to passwords?

b. Are passwords required to be changed at least every 90 days?

c. How many generations of passwords are maintained?

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

46. Is auditing enabled on the application?

a. What auditable events are set to be captured?

b. Is appropriate storage capacity given to audit records?

c. Are there alerts established to inform administrators of an audit processing failure?

i. How is the administrator alerted?

d. Does the application provide capabilities for monitoring, analyzing, and report generation of auditable events?

i. Does the reporting feature allow for reduction, so that reports on specific audit events can be tailored to a report?

e. Are time stamps used with each audit event?

f. How is the audit information protected?

g. How long are audit records maintained?

47. 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?

48. Does the Agency utilize the Plan of Actions and Milestones (POA&M) process to manage risks identified through security assessments or risk assessments?

49. Is a baseline configuration maintained for the application that contains software versions, patch levels, services used, etc.?

50. Does the Agency follow a configuration change control process?

a. How are change requests submitted?

b. Who analyzes the requests?

c. Is there an established Configuration Control Board that is involved in the approval process?

d. Are all changes to the information system documented?

51. Is there a list of personnel who are authorized to make changes to the application?

a. Is this list of personnel periodically reviewed?

52. Does the Agency have an implemented Incident Response process?

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

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

53. Are Risk Assessments conducted with results documented?

a. How often are Risk Assessments conducted?

b. What is the date of the last Risk Assessment?

54. Is the application managed using a System Development Life Cycle (SDLC) methodology that is consistent with NIST SP 800-64?

55. Is a list of prohibited/restricted functions, ports, protocols, and services identified and maintained?

56. Is a component inventory maintained to track all network assets?
- a. What elements are captured in the inventory? (e.g. manufacturer, model number, serial number, software license information, owner, etc.)
57. Is there a disaster recovery site or alternate processing facility?
- a. Are failover tests conducted and how often?
    - i. What is the date of the last test?
58. What software and version is used for Virus Protection?
59. What software and version is used for Intrusion Detection?
60. What software and version is used for Spam/Spyware Protection?
61. Does network traffic utilize encryption?
- a. Explain the type of encryption used.
62. What tools, to include their purpose, are used to perform network and system maintenance?
63. Is remote maintenance performed?

a. How are the remote maintenance sessions protected?

64. Is a list of personnel authorized to perform maintenance maintained?

65. Is there an established Rules of Behavior that describes user responsibilities and expected behavior?

a. Are users required to read and sign a statement (that's kept on file) indicating acknowledgement?

66. Are vulnerability scans conducted on the network?

a. What software is used for vulnerability scanning?

b. How often are vulnerability scans conducted?

c. Are the results of the vulnerability scans maintained?

d. When was the last vulnerability scan conducted?

67. Is there a list of software that is prohibited from used maintained?

68. Are there usage restrictions on mobile code (Java, JavaScript, ActiveX, Postscript, Shockwave, Flash, and VBscript)?

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

Draft