**Security and Confidentiality Questionnaire and Required Documents**

**Required documents:**

* Network diagrams.
* Data flow diagram.
* Security policies.
* Security risk assessment, SAS70.
* Building layout.

Vendor Name:

What type of data is being exchanged?

**General factors:**

# 1: Did you receive a copy of the Department of Revenue Services (DRS) Data Security Requirements as part of the state contract packet?

**Answer:**

# 2: How long have you been in the business of providing this type of service?

**Answer:**

# 3: Are you currently approved for use by any other state or federal taxing authority?

**Answer:**

# 4: At what address will you conduct this work?

**Answer:**

**City:**

**State:**

**Zip code:**

# 5: What are the MapQuest travel miles from the DRS, 450 Columbus Blvd, Hartford, CT 06103 to your operating location?

**Answer:**

# 6: How many reportable incidents are on file for your company within last 24 months?

**Answer:**

# 7: Have these incidents been self-reported by you?

**Answer:**

# 8: Do you have a formal risk assessment policy? If so, please provide.

**Answer:**

# 9: Do you provide similar services to other customers/agencies at this same location?

**Answer:**

# 10: Do you have a formal information security policy? If so, please provide.

**Answer:**

# 11: Is it a shared facility? If so, how are you separated? Are there common areas?

**Answer:**

**Personnel factors:**

# 12: Are your data security policies communicated to employees and acknowledgement forms signed?

**Answer:**

# 13: Is there a formal security awareness training program for all employees including temporary employees?

**Answer:**

# 14: Do subcontractors have any contact with DRS data? If yes, please give details.

**Answer:**

# 15: Do temporary employees have any contact with DRS data?

**Answer:**

# 16: Please describe your hiring practices. At what level are background checks performed; state/national level? Does it include a fingerprint-based criminal record check? What would preclude an applicant from being hired?

**Answer:**

# 17: What is your termination procedure? Do you conduct an exit interview?

**Answer:**

# 18: Are confidentiality agreements and/or non disclosure agreements required of all employees?

**Answer:**

# 19: Are employees issued a photo ID badge?

**Answer:**

# 20: Do personnel files include a copy of the employee photo?

**Answer:**

# 21: Do you enforce a "clean desk" policy throughout the facility?

**Answer:**

**Physical site security factors:**

# 22: Do you have security guards on-site? If so, what are their hours?

**Answer:**

# 23: Does the location have controlled entry, including key & combination control? If yes, who issues the access and are they logged? How long is log kept?

**Answer:**

# 24: Is there a loading dock at the facility? If so, is it kept locked? Who has access to the loading dock? Are there 24 hour cameras? If yes, how long are the tapes kept?

**Answer:**

# 25: What security measures are in place to safeguard DRS information when it is being worked on for both paper and electronic information?

**Answer:**

# 26: Is there a visitor log and are visitor badges issued? What kind of ID is needed by visitors? Who keeps the log and for how long?

**Answer:**

# 27: How is the facility secured when not occupied? Is there an alarm system? Are there cameras? Is it a closed or open circuit? Is there a monitoring system for fire?

**Answer:**

# 28: Who monitors the cameras? Are they tested? How long is film kept?

**Answer:**

# 29: Who is your transportation provider and do they meet our requirements as specified in our Data Security Document packet?

**Answer:**

**Logical security factors:**

# 30: Is there a documented asset management program?

**Answer:**

# 31: Is there an inventory of hardware/software assets? If so, please provide a copy of your hardware assets including make, model and serial number.

**Answer:**

# 32: What are the procedures for the disposal and/or destruction of physical media (e.g., paper documents, CDs, DVDs, tapes, disk drives, etc.)?

**Answer:**

**Data Security factors:**

# 33: What kind of data do you process? Electronic, paper, or both?

**Answer:**

# 34: Does the physical transport of DRS data (paper/media) meet transportation requirements including locked box/physical barrier, inventory control, cell phone availability, and 2 drivers on trips >2 hours?

**Answer:**

# 35: How is DRS data (paper/media) physically secured during storage?

**Answer:**

# 36: Is electronic DRS data stored on secure network drives, segregated from all other client or contractor data?

**Answer:**

# 37: Is access to DRS data restricted to a need-to-know, and only as required for the job?

**Answer:**

# 38: Describe your destruction policies, paper, electronic, computer servers, mobile devices, back up devices, microfiche, CD's - NIST compliant

**Answer:**

# 39: Is DRS data ever used in the test, development or QA environments?

**Answer:**

# 40: Is DRS data adequately protected from cleaning staff and maintenance/service staff?

**Answer:**

# 41: Please describe your work flow and provide a network diagram detailing this flow and the security features that are in place.

**Answer:**

**DRS Information Technology Department Security Review Questions   
Logical Data Security**

# 42 Please describe your process for receiving, storing and transmitting DRS electronic tax return information.

**Answer:**

# 43 Please describe the security controls that are utilized to transmitting DRS electronic data.

**Answer:**

# 44: Will your company ensure that access to DRS data is granted on a strict need-to know basis? How will this be accomplished?

**Answer:**

# 45: Will your company have the capabilities to encrypt DRS data when at rest (when not being modified or processed)? Will the data be encrypted when at rest? To what standard will the data be encrypted?

**Answer:**

# 46: What security measures do you have in place to secure DRS information when it is in transit (being transmitted)? Is the data encrypted? To what standard will the data be encrypted?

**Answer:**

# 47: Will your company grant access to our data based on the minimum access required to fulfill their job responsibilities and only for the period of time needed?

**Answer:**

# 48: Will an electronic DRS data stored on secure network drives be segmented from all other client data? How will this being accomplished?

**Answer:**

# 49: Will DRS data ever be used in Test, Development or QC environments?

**Answer:**

# 50: Will your company collect, maintain and periodically review detailed activity logs related to DRS data access?

**Answer:**

# 51: Will your company mitigate issues found when reviewing activity logs and report them to DRS in a timely manner?

**Answer:**

# 52: Will your company make available to the DRS, upon request, any log files and any research/supporting documentation relative to DRS data?

**Answer:**

# 53: Will your company collect, maintain and periodically review detailed system administrator activity logs for appropriateness related to DRS data?

**Answer:**

# 54: Do procedures used to grant and change access privileges require the approval of a supervisor or manager?

**Answer:**

# 54: What methods of authentication will be used to protect DRS data?

**Answer:**

# 56: Will you require all staff to have unique login names for all systems processing DRS data?

**Answer:**

# 57: What criteria are used to increase the security of user passwords for users that will be granted access to CT data?

* + Strong Passwords
  + Require password changes every 45 days
  + Requiring at least 8 character passwords
  + Prohibit the use of the last 6 passwords
  + Lock out user accounts after 3 failed attempts
  + System controlled hours of access
  + Procedures to verify user identity prior to password reset
  + Other

**Answer:**

# 58: What processes are in place for resetting passwords? Who has the capability to reset passwords?

**Answer:**

# 59: Do you have a policy prohibiting users from sharing passwords?

**Answer:**

**Computer Data Security**

# 60: Will your company have written computer security policies and procedures that users with access to DRS data will follow?

**Answer:**

61: Will your company provide physical security for all computers containing or accessing DRS data?  
**Answer:**

# 62: Will your company display a security banner reminding users of penalties for unauthorized inspection and/or disclosure prior to them accessing DRS data?

**Answer:**

# 63: Does your company prevent screen print capability?

**Answer:**

# 64: Does your company disable data storage on all local drives (A, B, C, etc.)?

**Answer:**

# 65: Does your company enforce a policy prohibiting the use of USB drives?

**Answer:**

# 66: Does your configure all computers to automatically lock after 5 minutes of inactivity?

**Answer:**

# 67: Will your company provide an immediate manual method of locking the desktop and have procedures in place requiring users of DRS data to utilize this function when leaving their workstation unattended?

**Answer:**

# 68: Do system administrators subscribe to security alert services such as CERT, Secunia, Microsoft, etc? Which ones?

**Answer:**

# 69: Will your company use antivirus software on all systems with access to DRS data with updated virus definitions applied at least weekly?

**Answer:**

# 70: What Operating Systems will be used for servers and workstations?

**Answer:**

# 71: Does your company have policies and procedures for applying server and workstation security updates?

**Answer:**

# 72: Do you have policies and procedures for reviewing and applying major application security updates?

**Answer:**

# 73: How will users of DRS data be granted access to that data?

**Answer:**

# 74: How will system administrators be granted access to DRS data?

**Answer:**

# 75: How will users and system administrators that do not require access to DRS data be prevented from gaining unauthorized access?

**Answer:**

# 76: Will DRS data be stored and used on a dedicated server or system?

**Answer:**

# 77: Will DRS data be stored and used on a dedicated physical hard drive?

**Answer:**

# 78: Will DRS data be stored and used on a disk array or SAN?

**Answer:**

# 79: How will your company securely delete/erase/wipe DRS data from your system at the end of the contract?

**Answer:**

# 80: Do you have a media sanitation/destruction policy and procedures related to electronic media including: all hard drives (including those under vendor maintenance), servers, mobile storage devices, backup media, CD/DVDs, USB, etc.

**Answer:**

# 81: Will there a system inventory log of equipment used to store, process, share, transmit or delete any DRS data?

**Answer:**

#82: Will the log include equipment make, model, serial number, description, location?

**Answer:**

# 83: Will there be a log maintained which documents changes to systems that contain DRS data?

**Answer:**

**Network Data Security**

# 84: Has your company ever provided a network diagram which includes all devices that will store, process, share, transmit or delete DRS data including all relevant security devices such as firewalls, routers, IDS, VLANS, switches, hubs, servers, workstations for DRS’s review and evaluation?

**Answer:**

# 85: Has your company provided a DRS data flow diagram to show the flow of CT data from cradle to grave?

**Answer:**

# 86: Are all network services hardware devices protected by physical security and require restricted access?

**Answer:**

# 87: Are all network services hardware devices protected by a strong authentication and is access restricted to network administrators only?

**Answer:**

# 88: Are all network services hardware devices accessed via tools that encrypt communications such as SSH or SNMPv3?

**Answer:**

# 89: Are insecure management protocols disabled on all network services hardware devices (ex. SNMPv1 and telnet)?

**Answer:**

# 90: Can network services hardware devices be managed remotely and if so, what security measures are in place to protect against unauthorized access, DoS or malicious attacks?

**Answer:**

# 91: Will router ACLs, firewall rules and switch configurations designed security to protect DRS data from unauthorized access? Please provide details.

**Answer:**

# 92: The use of wireless networks to access DRS data is prohibited outside of the facility. Does your company utilize wireless networks at this location?

**Answer:**

# 93: How are wireless networks secured to prevent unauthorized access or attacks on CT data? Is wireless traffic bound for your internal networks protected by a firewall? Is wireless traffic encrypted? With which protocol?

**Answer:**

# 94: Remote access to CT data is prohibited. Will your company utilize remote access into the environment containing DRS data?

**Answer:**

# 95: How will remote access connections secured to prevent unauthorized access to DRS data?

**Answer:**

# 96: Is your LAN network traffic encrypted? If not, are there other controls in place preventing unauthorized access to DRS data (ex. Switched network, restricted physical access to switches and network cabling, etc.)

**Answer:**

# 97: Is WAN network traffic encrypted when transferring DRS data?

**Answer:**

# 98: Are mobile computing devices (laptop, PDA, iPhones, etc.) used or allowed at your site?

**Answer:**

Rev. 8/2019