Department of Revenue Services

Requirements for Safeguarding Confidential Taxpayer Information

The Department of Revenue Services is entrusted with information that is among the most sensitive in government. It is critical that we safeguard and maintain the confidentiality of tax return and tax return information, as well as confidential information received from other agencies whether it is State or Federal data. As a Contractor with the Department of Revenue Services you too will be entrusted with safeguarding and maintaining the confidentiality of this information. Failure to do so may result in the cancellation of the contract and/or potential criminal prosecution.

The attached documents are the requirements for safeguarding confidential taxpayer information. This explains what the DRS regards as confidential information. It requires acknowledgement of awareness training and that all contractors understand the policies, procedures and penalties.

Table of Contents

- Policy for Access to and Safeguarding of DRS Confidential or Restricted Data by Contractors …pages 3-5

- Additional Contractor Requirements...pages 5 - 7

- Internal Revenue Service Exhibit 7 an IRS requirement for all contractors….pages 8-14

- Definitions…pages 15 & 16

- An Annual Reminder of the Disclosure and Inspection Rules and Procedures for State and Federal Tax Return Information. ...pages 17-19

- Acknowledgement Form…page 20

- Disclosure of Tax Information form…page 21

- Monthly required Security Measure Check List…page 22

- Security and Confidentiality Questionnaire and required Documents…pages 23-35

Policy for Access to and Safeguarding of DRS Confidential or Restricted Data by Contractors

Policy Number: P-4001
Version: 1.**3**
Date Issued (revised): Nov 2017
Date Effective: immediately

Purpose

This Policy outlines the confidentiality and security requirements for Contractors of the State of Connecticut, as part of their contractual relationship, are authorized to access and view DRS confidential or restricted data.

Scope

This policy covers all DRS contractors, who as part of their contractual relationship, are authorized to have access to DRS confidential or restricted data or DRS technology systems.

Should a conflict exist between this policy and a State-wide policy, the more restrictive policy would take precedence.

Authority

The Security Review Committee (SRC) is responsible for developing, implementing and enforcing policies that regulate the storage, access to, and use of confidential and restricted data.

Policy Statements

1. Before accessing, in any manner, any DRS confidential or restricted data, each contractor will confirm that it has read and understands the DRS/IRS confidentiality requirements material. The Contractor will be provided with a copy of the DRS "Requirements for Safeguarding Confidential Taxpayer Information". Each of the Contractor's employees who may come in contact with DRS confidential or restricted data must confirm that he or she has viewed and understands the confidentiality requirements.

2. Except as provided herein, contractors who are working on site at a DRS location, will be required to utilize only DRS supplied equipment to connect to DRS technology systems. If DRS determines that access to its technology systems is necessary to fulfill the contractor's obligations under the contract and the contract provides for such access, the Date Security Officer, in consultation with the Information Services Division (ISD) Director, shall determine in what manner and under what conditions will such access be provided. The Date Security Officer will also determine what, if any, non-DRS equipment will be allowed to access or store DRS confidential or restricted data. The Contractor will provide the designated equipment for

inspection before connection to the DRS technology systems. Additionally, such equipment will be subject to additional inspections as deemed necessary by the Data Security Officer. The following conditions must be met in order for Contractor's equipment to be allowed access to the DRS technology systems:

a. Contractor's computer equipment must be virus free and loaded with the most current version of anti-virus software
b. Contractor will agree to install software and configure software and hardware on its equipment as is required by the DRS.
c. Contractor will agree to restrictions on the removal of its equipment from DRS premises as determined by the Date Security Officer.
d. Contractor will agree to requirements for locking and/or securing of its equipment.

3. For contractors whose contract provides for remote access to the DRS technology systems, the Date Security Officer, in consultation with the ISD Director, shall determine in what manner and under what conditions such access will be allowed. The Date Security Officer will determine what equipment of the Contractor will be allowed to access or store DRS confidential or restricted data. Such equipment will be made available for inspection by the Data Security Officer prior to connection to the DRS technology systems and will be subject to additional inspections as deemed necessary. The following conditions must be met in order for Contractor's equipment to be allowed access to the DRS technology systems:

   a. Contractor's computer equipment must be virus free and loaded with the most current version of anti-virus software
   b. Contractor will agree to install software and configure software and hardware on its equipment.
   c. Contractor will agree to requirements for locking and/or securing of its equipment.

4. On DRS supplied equipment, the DRS may install software that will be required to remain on such equipment until the project has been completed and a final inspection of such equipment has been conducted.

5. DRS may disable all USB ports, storage saving and transfer devices from the DRS supplied equipment provided to Contractor. Should there be a need to transfer information the Contractor shall follow procedures established by the DRS.

6. The use of Flash Drives and other media used by Contractors to store or transfer DRS confidential or restricted data is prohibited.

7. All requirements pertaining to the access of DRS confidential or restricted data, including, but not limited to, the method and location of storage, safeguarding and destruction will be determined solely by the DRS.

8. Contractors will provide DRS with their policies regarding:

    a. Replacing/recycling personal computers and Multi-Functional Printing devices
    b. Remote access
    c. Restrictions or prohibitions on the storing or transfer of client information
    d. Employee termination procedures (including exit checklists)
    e. Procedures for violation of Contractor's policies
    f. Process used to conduct any required background checks.

When applicable, the Contractor, will provide the DRS Data Security Team with a written inventory of all DRS confidential or restricted information currently in its possession. The Contractor, or its individual employees, will be required to sign the inventory document attesting to its accuracy.

9. Lost or stolen keys, fobs , access codes, badges or any other item that are used in connection with any DRS assignment will be immediately reported using the protocol provided .

10. For Contractors who are working on site at a DRS location, the Contractor will inform the Data Security Officer at least 5 business days prior to a Contractor's employee leaving the DRS assignment. In no case shall such employee leave DRS without the Contractor's equipment being inspected as determined by the DRS Information Services Division. Once the review has been completed, such employee will not be allowed to connect to any DRS technology systems or store any DRS confidential or restricted data on the previously inspected equipment.

11. Any Contractor who has access to or is in possession of DRS confidential or restricted data must comply with all provisions of the State of Connecticut Security for Mobile Computing and Storage Devices Policy.

12. Vendor must allow for inspections by DRS internal audit staff as well as the State of Connecticut Auditors of Public Accounts. The State reserves the right to inspect the facility of the vendor and/or subcontractor(s) approved by DRS before an award is made and anytime during the contract period.

13. Prior to working on site at a DRS location, a Contractor must disable all wireless internet and communication capabilities on its equipment. Additionally, throughout the period of its contract, the Contractor must be prepared to demonstrate to the DRS Information Services Division that such capabilities remain disabled.

14. All vendor and subcontractor employees, on-site or off-site, who perform functions that put them in contact with State of Connecticut tax returns or tax return information, must sign a Department of Revenue Services confidentiality statement.

Additional Contractor Requirements

The contractor must provide a detailed document outlining contractors process and quality control measures that are in place prior to the start of his contract and maintained throughout the contract.

All DRS information in the vendor possession must be documented and remain in a secure location within the Continental United States. All electronic information must remain encrypted when at rest or not in use. DRS information shall not be commingled with any other information.

The contractor will pay for losses that are sustained as a result of acts committed by the contractor, the contractors' staff or its subcontractors. The contractor will pay for losses resulting from dishonesty acts committed by the contractor, the contractors' staff or its subcontractors. It is the contractors' responsibility to safeguard DRS information while it is in the contractors' possession. If there is a security breach that affects DRS information while that information is in the possession of the contractor, the contractor will pay for all costs incurred with that security breach. This will include but not be limited to credit protection for all affected taxpayers for a minimum of 2 years and all expenses incurred by the State of Connecticut in connection with the security breach. It is the contractor's responsibility to immediately notify the Department of Administrative Services @ (860) 713-5627-2300, the Department of Revenue Services @ (860) 297-4900 and Jonathan Reid (860) 297-4800 as soon as a loss or breach of DRS information is suspected.

All vendor and subcontractor employees, on-site or off-site, who performs functions that put them in contact with State of Connecticut tax returns or tax return information must sign a Department of Revenue Services confidentiality statement. In addition, a background check must be performed on anyone who has access to the tax returns or tax return information, this should include on both state and national level and may require fingerprinting. The background checks are the responsibility of the vendor and the subcontractor including all costs associated there with. If the vendor's process is determined by DRS to be sufficient to protect the identity and confidentiality of the taxpayer the vendor may request that some of the background check requirements be waived. This must be approved in writing by DRS. DRS has the right to request proof that the background check has been conducted. Notwithstanding the aforementioned provisions of this paragraph, any vendor, subcontractor or employee of the vendor or subcontractor who has been convicted of a tax crime, embezzlement, forgery or other financial crimes or offences that pertain to or involve a fiduciary trust or responsibility is prohibited or ineligible from working with any part of this contract.

The vendor must provide a security plan which establishes their auditing and logging capabilities utilizing the following requirements: 1. All transaction access to the DRS Information must be logged and maintained for the period legally required based upon the information being accessed. 2. The contractor must house and maintain these logs. 3. If requested by the DRS, the contractor will be required to provide state and federal auditors and authorized employee's access to the logs

If determined necessary by the DRS Data Security Team the vendor will submit a completed monthly "Security Measures Checklist" to the DRS Data Security Team. The checklist will be developed by DRS once the company's facility is inspected and process for completing the contract is approved.

All DRS information must be expunged at the end of the contract. The Contractor will get approval from the DRS to and will document the process and certify that all DRS data was expunged. The contractor will certify that the data will be destroyed on site by individuals who have been previously approved by DRS to have access to the DRS Information and will utilize the NIST 800-88 approved destruction methodology. The contractor must provide evidence that it has the capabilities in place to assure that DRS will be notified and has approved the destruction or relocation of all equipment used by the contractor during the term of the contract. Prior to destroying or sending the equipment containing DRS information off-site, the contractor must certify, in writing, that it has wiped all electronic media capable of storing the DRS Information.

The vendor must have appropriate equipment and personnel to meet the contract requirements. If it is found that the vendor is not qualified to perform the work as specified, the State has the right to seek reimbursement from the vendor for the inspection. This includes ALL costs, such as airfare, car rental, hotel, meals and the salary of the individuals(s) performing the site inspection. The right is also reserved to inspect work in progress at any time. Part of the inspection will require the vendor to show its ability to maintain security of all materials in a manner satisfactory to the Department of Revenue Services.

The vendor and any subcontractor(s) approved by DRS must have working fire suppressant and security systems on-site, which must meet the approval of the Agency at the time of the initial inspection, and be maintained throughout the contract period. The vendor must submit proof, such as inspection certificates, in regards to working fire and security systems.

SUBCONTRACT

Subcontracting any DRS information in connection with this contract is prohibited without prior written approval form DRS. When subcontracting may be permitted, it is understood and agreed that the vendor shall not assign, transfer, convey, sublet or otherwise dispose of their contract or their right of title, or portion thereof, to any person, firm or corporation without previous written consent of the Connecticut Department of Revenue Services and the Connecticut Department of Administrative Services. Failure to do so is cause for cancellation of the contract.

Contractor must abide by the following Internal Revenue Requirements:

Safeguarding Contract Language Exhibit 7

Exhibit 7 *Safeguarding Contract Language*

CONTRACT LANGUAGE FOR GENERAL SERVICES

!. **PERFORMANCE**

In performance of this contract, the Contractor agrees to comply with and assume responsibility for compliance by his or her employees with the following requirements:

(1) All work will be performed under the supervision of the contractor or the contractor's responsible employees.

(2) The contractor and the contractor's employees with access to or who use FTI must meet the background check requirements defined in IRS Publication 1075.

(3) Any Federal tax returns or return information (hereafter referred to as returns or return information) made available shall be used only for the purpose of carrying out the provisions of this contract. Information contained in such material shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of this contract. Inspection by or disclosure to anyone other than an officer or employee of the contractor is prohibited.

(4) All returns and return information will be accounted for upon receipt and properly stored before, during, and after processing. In addition, all related output and products will be given the same level of protection as required for the source material.

(5) No work involving returns and return information furnished under this contract will be subcontracted without prior written approval of the IRS.

(6) The contractor will maintain a list of employees authorized access. Such list will be provided to the agency and, upon request, to the IRS reviewing office.

(7) The agency will have the right to void the contract if the contractor fails to provide the safeguards described above.

(8) (Include any additional safeguards that may be appropriate.)

II. CRIMINAL/CIVIL SANCTIONS

(1) Each officer or employee of any person to whom returns or return information is or may be disclosed shall be notified in writing by such person that returns or return information disclosed to such officer or employee can be used only for a purpose and to the extent authorized herein, and that further disclosure of any such returns or return information for a purpose or to an extent unauthorized herein constitutes a felony punishable upon conviction by a fine of as much as $5,000 or imprisonment for as long as five years, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee

that any such unauthorized future disclosure of returns or return information may also result in an award of civil damages against the officer or employee in an amount not less than $1,000 with respect to each instance of unauthorized disclosure. These penalties are prescribed by IRCs 7213 and 7431 and set forth at 26 CFR 301.6103(n)-1.

(2) Each officer or employee of any person to whom returns or return information is or may be disclosed shall be notified in writing by such person that any return or return information made available in any format shall be used only for the purpose of carrying out the provisions of this contract. Information contained in such material shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of this contract. Inspection by or disclosure to anyone without an official need-to-know constitutes a criminal misdemeanor punishable upon conviction by a fine of as much as $1,000.00 or imprisonment for as long as 1 year, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized inspection or disclosure of returns or return information may also result in an award of civil damages against the officer or employee [United States for Federal employees] in an amount equal to the sum of the greater of $1,000.00 for each act of unauthorized inspection or disclosure with respect to which such defendant is found liable or the sum of the actual damages sustained by the plaintiff as a result of such unauthorized inspection or disclosure plus in the case of a willful inspection or disclosure which is the result of gross negligence, punitive damages, plus the costs of the action. The penalties are prescribed by IRCs 7213A and 7431 and set forth at 26 CFR 301.6103(n)-1.

(3) Additionally, it is incumbent upon the contractor to inform its officers and employees of the penalties for improper disclosure imposed by the Privacy Act of 1974, 5 U.S.C. 552a. Specifically, 5 U.S.C. 552a(i)(1), which is made applicable to contractors by 5 U.S.C. 552a(m)(1), provides that any officer or employee of a contractor, who by virtue of his/her employment or official position, has possession of or access to agency records which contain individually identifiable information, the disclosure of which is prohibited by the Privacy Act or regulations established thereunder, and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than $5,000.

(4) Granting a contractor access to FTI must be preceded by certifying that each individual understands the agency's security policy and procedures for safeguarding IRS information. Contractors must maintain their authorization to access FTI through annual recertification. The initial certification and recertification must be documented and placed in the agency's files for review. As part of the certification and at least annually afterwards, contractors must be advised of the provisions of IRCs 7431, 7213, and 7213A (see Exhibit 4. *Sanctions for Unauthorized Disclosure*. and Exhibit 5, *Civil Damages for Unauthorized Disclosure).* The training provided before the initial certification and annually thereafter must also cover the incident response policy and procedure for reporting unauthorized disclosures and data breaches. (See Section 10) For both the initial certification and the annual certification, the contractor must sign, either with ink or electronic signature, a confidentiality statement certifying their understanding of the security requirements.

Ill. INSPECTION

The IRS and the Agency, with 24 hour notice, shall have the right to send its inspectors into the offices and plants of the contractor to inspect facilities and operations performing any work with **FTI** under this contract for compliance with requirements defined in IRS Publication 1075. The IRS' right of inspection shall include the use of manual and/or automated scanning tools to perform compliance and vulnerability assessments of information technology (IT) assets that access, store, process or transmit FTI. On the basis of such inspection, corrective actions may be required in cases where the contractor is found to be noncompliant with contract safeguards.

Safeguarding Contract Language **Exhibit 7**

CONTRACT LANGUAGE FOR TECHNOLOGY SERVICES

!. PERFORMANCE

In performance of this contract, the contractor agrees to comply with and assume responsibility for compliance by his or her employees with the following requirements:

(1) All work will be done under the supervision of the contractor or the contractor's employees.

(2) The contractor and the contractor's employees with access to or who use FTI must meet the background check requirements defined in IRS Publication 1075.

(3) Any return or return information made available in any format shall be used only for the purpose of carrying out the provisions of this contract. Information contained in such material will be treated as confidential and will not be divulged or made known in any manner to any person except as may be necessary in the performance of this contract. Disclosure to anyone other than an officer or employee of the contractor will be prohibited.

(4) All returns and return information will be accounted for upon receipt and properly stored before, during, and after processing. In addition, all related output will be given the same level of protection as required for the source material.

(5) The contractor certifies that the data processed during the performance of this contract will be completely purged from all data storage components of his or her computer facility, and no output will be retained by the contractor at the time the work is completed. If immediate purging of all data storage components is not possible, the contractor certifies that any IRS data remaining in any storage component will be safeguarded to prevent unauthorized disclosures.

(6) Any spoilage or any intermediate hard copy printout that may result during the processing of IRS data will be given to the agency or his or her designee. When this is not possible, the contractor will be responsible for the destruction of the spoilage or any intermediate hard copy printouts, and will provide the agency or his or her designee with a statement containing the date of destruction, description of material destroyed, and the method used.

(7) All computer systems receiving, processing, storing or transmitting FTI must meet the requirements defined in IRS Publication 1075. To meet functional and assurance requirements, the security features of the environment must provide for the managerial, operational, and technical controls. All security features must be available and activated to protect against unauthorized use of and access to Federal Tax Information.

(8) No work involving Federal Tax Information furnished under this contract will be subcontracted without prior written approval of the IRS.
Publication 1075 (September 2016) Page 144

(9) The contractor will maintain a list of employees authorized access. Such list will be provided to the agency and, upon request, to the IRS reviewing office.(10) The agency will have the right to void the contract if the contractor fails to provide the safeguards described above.

(10) (Include any additional safeguards that may be appropriate.)

II. CRIMINAL/CIVIL SANCTIONS

(1) Each officer or employee of any person to whom returns or return information is or may be disclosed will be notified in writing by such person that returns or return information disclosed to such officer or employee can be used only for a purpose and to the extent authorized herein, and that further disclosure of any such returns or return information for a purpose or to an extent unauthorized herein constitutes a felony punishable upon conviction by a fine of as much as $5,000 or imprisonment for as long as 5 years, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized further disclosure of returns or return information may also result in an award of civil damages against the officer or employee in an amount not less than $1,000 with respect to each instance of unauthorized disclosure. These penalties are prescribed by IRCs 7213 and 7431 and set forth at 26 CFR 301.6103(n)-1.

(2) Each officer or employee of any person to whom returns or return information is or may be disclosed shall be notified in writing by such person that any return or return information made available in any format shall be used only for the purpose of carrying out the provisions of this contract. Information contained in such material shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of the contract. Inspection by or disclosure to anyone without an official need-toknow constitutes a criminal misdemeanor punishable upon conviction by a fine of as much as $1,000 or imprisonment for as long as 1 year, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized inspection or disclosure of returns or return information may also result in an award of civil damages against the officer or employee [United States for Federal employees] in an amount equal to the sum of the greater of $1,000 for each act of unauthorized inspection or disclosure with respect to which such defendant is found liable or the sum of the actual damages sustained by Hie plaintiff as a result of such unauthorized inspection or disclosure plus in the case of a willful inspection or disclosure which is the result of gross negligence, punitive damages, plus the costs of the action. These penalties are prescribed by IRC 7213A and 7431 and set forth at 26 CFR 301.6103(n)-1.

(3) Additionally, it is incumbent upon the contractor to inform its officers and employees of the penalties for improper disclosure imposed by the Privacy Act of 1974, 5 U.S.C. 552a. Specifically, 5 U.S.C. 552a(i)(1), which is made applicable to contractors by 5 U.S.C. 552a(m)(1), provides that any officer or employee of a contractor, who by virtue of his/her employment or official position, has possession of or access to agency records which contain individually identifiable information, the disclosure of which is prohibited by the Privacy Act or regulations established thereunder, and who knowing that disclosure of the specific material is prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than $5,000.

(4) Granting a contractor access to FTI must be preceded by certifying that each individual understands the agency's security policy and procedures for safeguarding IRS information. Contractors must maintain their authorization to access FTI through annual recertification. The initial certification and recertification must be documented and placed in the agency's files for review. As part of the certification and at least annually afterwards, contractors must be advised of the provisions of IRCs 7431, 7213, and 7213A {see *Exhibit 4. Sanctions for Unauthorized Disclosure,* and *Exhibit* 5. *Civil Damages for Unauthorized* Disclosure). The training provided before the initial certification and annually thereafter must also cover the incident response policy and procedure for reporting unauthorized disclosures and data breaches. (See Section 10) For both the initial certification and the annual certification, the contractor must sign, either with ink or electronic signature; a confidentiality statement certifying their understanding of the security requirements.

III. INSPECTION

The IRS and the Agency, with 24 hour notice, shall have the right to send its inspectors into the offices and plants of the contractor to inspect facilities and operations performing any work with FTI under this contract for compliance with requirements defined in IRS Publication 1075. The IRS' right of inspection shall include the use of manual and/or automated scanning tools to perform compliance and vulnerability assessments of information technology (IT) assets that access, store, process or transmit FTI. On the basis of such inspection, corrective actions may be required in cases where the contractor is found to be noncompliant with contract safeguards.

Definitions

Contractor

Any individual or company that enters into any agreement either with the State of Connecticut or an Agency thereof to perform services. This includes all of the employees of this individual or company and any subcontractors that they may contract with.

Contractor's Equipment

Any equipment that the contractor uses in connection with the performance of the contract.

Requirements for Safeguarding Confidential Taxpayer Information

A packet that will guide and assist contractors in meeting their responsibilities to safeguard and protect DRS confidential and restricted information.

DRS Confidential or Restricted Data

Confidential or restricted State data includes but is not limited to;

Tax return or return information and/or personally identifiable information that is not in the public domain and if improperly disclosed could be used to steal an individual's identity, violate the individual's right to privacy or otherwise harm the individual;

Organizational information that is not in the public domain and if improperly disclosed might: cause a significant or severe degradation in mission capability; result in significant or major damage to organizational assets; result in significant or major financial loss; or result in significant, severe or catastrophic harm to individuals.

DRS/IRS Confidentiality Training Material

Shall include any material supplied to the contractor to guide them in the safeguarding of confidential taxpayer information.

DRS Location

Any facility or portion thereof, under the direct control of DRS, in which an agency function is performed. In certain cases, this definition can also include other State agencies and other DRS contracted vendors who, under the control of DRS, supply necessary support services.

DRS Supplied Equipment

Any equipment supplied by the State of Connecticut or any Agency thereof to any contractor performing services to DRS

DRS Technology Systems

Shall include computer hardware, software, firmware applications, information and communications pertaining to any State of Connecticut or an Agency thereof computer system or network.

Date Security Officer

The DRS employee designated by the Commissioner to act as the single point of contact between DAS and DRS for issues that relate to the State of Connecticut's policy on Data Storage, Security for Mobile Computing and Storage Devices.

19PSX0208
Exhibit E

DEPARTMENT OF REVENUE SERVICES
Administration Division
MEMORANDUM

DATE: August 13, 2019

TO: All DRS Contractors & Subcontractors

FROM: Mary Kate Harlow **TELEPHONE:** (860) 297-4967
Systems Control Officer

SUBJECT: Disclosure and inspection rules and procedures for state and federal tax return information

As Contractors or Subcontractors of the Department of Revenue Services, you may come in contact with information that is among the most sensitive in government. Therefore, it is critical that you maintain the confidentiality of tax return and tax return information, as well as confidential information received from other state and federal agencies you may come in contact with. The purpose of this memorandum is to remind you of the need for strict adherence to the following guidelines. Failure to comply with the confidentiality standards discussed below will result in actions by the Department of Revenue Services. Should the particular facts and circumstances warrant it, a violation may result in termination of the contract, potential criminal prosecution and civil monetary damages.

- Confidential tax information that you access must relate directly to your individual responsibilities as a Contractor or Subcontractor.

- Confidential information should never be in open view when you are transporting confidential documents and records outside of your work area.

- Confidential tax information may be discussed only with authorized individuals and shared with employees who have a specific business need for such information.

- All confidential tax information must be properly destroyed. Paper documents must be shredded to 5/16 – inch strips or cross shredded inserted in a perpendicular direction. Microfilm and Microfiche must be shredded to 1/35 –inch by 3/8 inch strips. After shredding has occurred it may be used for pulp and recycled.

- Confidential taxpayer information must not be stored on a mobile computing device or mobile storage device. The term "mobile computing device" refers to portable or mobile computing and telecommunications devices that can execute programs. This definition includes, but is not limited to notebooks, palmtops, BlackBerry devices, PDAs, IPods and cell phones with internet browsing capability. The term "mobile storage devices" includes but is not limited to, mobile computing devices, diskettes, magnetic tapes, external/removable hard drives, flash cards (e.g., SD, Compact Flash), thumb drives (USB keys), jump drives, compact disks, digital video disks, etc.

- "Inspection" (e.g. "browsing") or "Disclosure" of tax returns and tax return information by Contractors or Subcontractors of any Connecticut or federal agency, including former Contractors or Subcontractors who has or had access to returns or return information or any current for former officer or employee of any contractor or subcontractor, whether the contractor or subcontractor was involved in the processing, storage, transmission, or reproduction of returns or return information, the programming, maintenance, repair, testing, or procurement of equipment, or the providing of any other service to DRS is subject to the penalties stated in Conn. Gen Stat. §12-15.

In addition to complying with the general guidelines above, you are required to understand and adhere to the federal and state laws relative to the confidentiality of tax information listed below.

Penalties for Unlawful Disclosure or Inspection of State and Federal Tax Return Information

1. State Penalties

C.G.S. §12-15

(f) Returns and return information shall, without written request, be open to inspection by or disclosure to: (1) Officers and employees of the Department of Revenue Services whose official duties require such inspection or disclosure for tax administration purposes; (2) officers or employees of an agency or office in accordance with subdivision (1) or (13) of subsection (b) of this section whose official duties require such inspection; and (3) officers or employees of any person in accordance with subdivision (12) of subsection (b) of this section, whose duties require such inspection or disclosure.

(g) Any person who violates any provision of this section shall be fined not more than one thousand dollars or imprisoned not more than one year, or both.

2. Federal Penalties

In 1997, the U.S. Congress passed and the President signed into law H.R. 1226 known as the "Taxpayer Browsing Protection Act." The major impact of this bill was to include "inspection," i.e., "browsing," as subject to the kind of penalties that previously applied only to "disclosure." Within this bill inspection is defined as, "any examination of a return or return information." The second impact of this Bill is that a taxpayer shall be notified of any unauthorized disclosure or inspection of their return. Anyone making an unlawful disclosure or inspection of federal tax return information could be subject to the following penalties:

I. R. C. § 6103: Prohibits unauthorized disclosure of federal tax returns or return information by employees and former employees of state and IV-D agencies.

I. R. C. § 7213: Makes any unauthorized disclosure of federal tax returns or return information a felony punishable by a fine of up to $5,000 and/or imprisonment for not more than five years, together with the costs of prosecution.

I. R. C. § 7213A: Prohibits the unauthorized willful inspection ("browsing") of federal tax returns or return information and makes such inspection punishable by a fine of up to $1,000 and/or imprisonment for not more than one year, together with the costs of prosecution.

I. R. C. § 7431: Permits a taxpayer to bring a civil action for damages in a federal district court. Damages that can be brought would be the greater of $1,000 for each unauthorized disclosure or inspection or the actual damages sustained by the taxpayer, plus punitive damages.

Information obtained from other State Agencies

Any and all information received from other state agencies is regarded as Confidential Information and may not be redisclosed.

Reporting Improper Inspections or Disclosures

Upon suspecting or discovering a possible improper inspection or disclosure of tax information, including breaches and security incidents, the individual suspecting, making the observation or receiving the information must immediately contact Mary Kate Harlow, Systems Control Officer of the Administration Division at (860) 297-4967. Any incident that may contain FTI must be reported to the Treasury Inspector General for Tax Administration (TIGTA) and the IRS Office of Safeguards within 24 hours, we will contact these agencies concerning this matter.

If you are aware of any potential violations of the confidentiality statutes or the Department's policy governing unauthorized access, please refer this information immediately to the Department of Revenue Services Systems Control Officer listed above.

If you should have any questions regarding the use, disclosure, or inspection of the tax information, I can be reached at (860) 297-4967 or by email to mk.harlow@po.state.ct.us.

You should retain a copy of this memorandum either in electric or paper format for future reference. Attached is a form for you to sign as an acknowledgment that you have received, read and understand the standards governing the access to, and disclosure of, confidential information.

19PSX0208
Exhibit E

ACKNOWLEDGEMENT

I have read the **"**Disclosure and inspection rules and procedures for state and federal tax return information" by signing below I acknowledge that I and understand the procedures and penalties.

Company Name

Employee Name	Signature	Date	Title

STATE OF CONNECTICUT
DEPARTMENT OF REVENUE SERVICES
450 Columbus Blvd, HARTFORD, CT 06103

DISCLOSURE OF TAX INFORMATION

As an employee, agent or vendor of the Connecticut Department of Revenue Services, you may come in contact with state and/or federal tax returns, and tax return information. **All tax information, in whatever form, is strictly confidential**; and you may not disclose any such information during or after your employment or contract period with this Department. Unauthorized disclosure or inspection of any federal or state tax information may result in dismissal, criminal prosecution and civil suit as prescribed by federal and state statues. (**Connecticut General Statute 12-15 and 7213(A), 7431 of the Internal Revenue Code**.)

As an employee, agent or vendor of this Department, if there is any doubt as to what information can be furnished (even when persons represent themselves as the taxpayer), you should consult your supervisor or agency contact. **As an agent of this Department** unauthorized disclosure of a tax return or return information is prohibited.

I have read the above information on disclosure and inspection of tax return information and understand that this is a condition of employment or contract with this Department. Please sign and return to the **Department of Revenue Services; c/o Business Office-450 Columbus Blvd; Hartford, CT 06103.**

_____

Print Name

_____

Name of Company

_____

Signature **Date**

Security Measures Check List

1. DRS information is encrypted when at rest or not in use.	
2. Combinations, key pads and/or access codes are changed when employees are terminated.	
3. All doors and exits have been examined to verify that they are properly secured and locked.	
4. Rooms with computers containing DRS information are locked at the end of the day.	
5. Security cameras are in proper working order and the information is being recorded and saved for at least 30 days. The recordings have been inspected for quality purposes.	
6. The central alarm system is tested and in proper working order – this has been confirmed with the central monitoring station.	
7. Fire suppressant systems have been inspected for proper charge and leaks and tested quarterly or other predetermined time frame.	
8. All DRS information that has been printed is destroyed by shredding.	
9. There are no cameras or cell phones in the work area that DRS information is being worked on. An inspection of the area confirms this.	
10. A clean desk policy is being enforced.	
11. There is no remote access to any DRS information.	
12. Antivirus, server and desktop operating systems and application patches are current.	
13. Internet access is disabled from computers working on DRS information.	
14. Secure file transfer protocol is in use.	
15. DRS information is not co-mingled.	
16. Password Security Standards are in place o Requirement of password changes every 45 days o Requirement of at least 8 character passwords o Prohibition of the use of the last 6 passwords o Locking out user accounts after 3 failed attempts o Procedures to verify user identity prior to password reset o System controlled hours of access	
17. DRS has approved all Subcontracting of work that involves DRS data or contact with DRS data.	
18. Any DRS data that must be destroyed is done so following specific guidelines from DRS.	
19. All new staff or approved contractors have seen the IRS video and the DRS security requirements document and the signed acknowledgement was sent to DRS.	
20. New employees have had background checks conducted.	

Any requirement found deficient will be noted and discussed with DRS and the results will be attached to this document.
These steps were performed by _____Date _____.
Print Name _____