



Lindsey M. Stepp
Commissioner



Ora M. LeMere
Assistant Commissioner

State of New Hampshire Department of Revenue Administration

Vendor Onboarding Package – Non IT Component

Enclosed are the following onboarding forms and agreements as required by the New Hampshire Department of Revenue Administration (DRA):

- Non-Disclosure and Confidentiality Agreement
- Policy #22-001 Disclosures of Taxpayer and Department Information

NON-DISCLOSURE AND CONFIDENTIALITY AGREEMENT

In consideration for and as a condition of the contract between the State of New Hampshire Department of Revenue Administration (the "Department" and "NHDRA") and _____ ("Contractor"), dated as of _____, 20__, the ("Contract"), Contractor hereby agrees to hold and keep certain information confidential in accordance with the following terms and conditions of this agreement (the "Agreement"):

1. Contractor and Contractor's Representatives

When this Agreement refers to the "Contractor," "You," or "Your" it shall mean all of the officers, employees, agents and representatives of the Contractor and of any of its subcontractors¹ including those who work on the Contract as well as those who do not work on the Contract but may have the possibility of inadvertent access to Confidential Information (as defined below) as a result of having access to the Contractor's office space and/or computer systems.

2. Confidential Information

(a) As used herein, the term "Confidential Information" refers to (i) all records, files, and data of the DRA, unless subject to a specific exemption under RSA 21-J:14; (ii) all federal tax information ("FTI") in the possession of the NHDRA access to which is governed by Internal Revenue Code Sections 7213 and 7213A, the associated Treasury Regulations, and Internal Revenue Service Publication 1075; (iii) any and all other information concerning the NHDRA's business and affairs that may be provided or made available to You by the NHDRA and is not provided to the general public via the NHDRA's website or otherwise disseminated by the NHDRA to the general public; (iv) all notes, summaries, forecasts, analyses, compilations, studies, or other documents made by the Contractor, or received by the Contractor directly or indirectly from the NHDRA, not provided to the general public via the NHDRA's website or otherwise disseminated by the NHDRA to the general public in whatever form or storage medium, whether such information is or was provided prior to or subsequent to the date of this Agreement, whether or not such information is marked "Confidential" or bears a similar restrictive legend or other confidential designation.

(b) The definition of "Confidential Information" also shall include the information described in Exhibit A to NHDRA Policy No. 22-001, as amended on November 4, 2022 and as further amended from time to time, entitled "Confidential Information Contract Provisions" and which is attached hereto as Exhibit "A."

(c) The term "Confidential Information" does not include information which: (i) is disseminated to the general public by the NHDRA on the NHDRA website or via an alternate medium; (ii) would be available to the general public via a request for information pursuant to RSA 91-A; (iii)

¹ A Contractor who works for the NHDRA generally is not allowed to retain a subcontractor to work on the NHDRA's project unless approved in advance by the NHDRA.

NON-DISCLOSURE AND CONFIDENTIALITY AGREEMENT

was available to Contractor on a non-confidential basis prior to gaining access to it as a result of the Contract; or (iv) was independently developed by Contractor without the use of or reference to any Confidential Information.

3. Permitted Use and Non-Disclosure of Confidential Information.

Contractor agrees that the Contractor shall use all Confidential Information solely for the purpose of work performing the Contract, and for no other purpose whatsoever. Contractor agrees that the Contractor shall keep the Confidential Information confidential and shall not disclose any of the Confidential Information to anyone; provided, however, that disclosure of such information may be made by Contractor to any of its employees or representatives who are actively and directly participating in performance of the Contract and who need to know such information. It is understood and agreed that Contractor shall cause each such employee or representative to treat such information as Confidential Information and comply with the terms of this Agreement as if such employee or representative were a party to this Agreement, and that Contractor shall be responsible to the NHDRA for any breach of the provisions hereof by any such employee or representative.

4. Obligation to Report to NHDRA Any Unauthorized Access or Disclosure of Confidential Information

In the event of any unauthorized access, use or disclosure of Confidential Information, the Contractor shall immediately notify the NHDRA both orally and in writing. Any such unauthorized access, use or disclosure of Confidential Information is an Event of Default upon which the NHDRA may decide to discipline the Contractor and keep the Contract or may immediately treat the Contract as breached and pursue any remedies at law or in equity or in both. In the event the NHDRA treats the Contract as breached, all provisions of this Agreement remain in full force and effect with NHDRA retaining all rights to enforce the same in equity or law.

5. Return, Destruction, or Retention of Confidential Information.

Upon completion of the Contract or at any time upon written request of the NHDRA, Contractor shall promptly return or destroy all Confidential Information along with all copies of the same. In all cases of destruction, Contractor shall promptly provide to the NHDRA certified written notice of such destruction. Notwithstanding the foregoing, Contractor may keep (a) copies of the Confidential Information to the extent required by law, rule, regulation, or administrative order, and (b) backup copies of items containing or constituting Confidential Information in computer systems to the extent that routine computer backup procedures or processes create such copies. Any such retained Confidential Information shall continue to be subject to all obligations of confidentiality set forth in this Agreement until such Confidential Information has been returned or destroyed as set forth in this section, and such Confidential Information shall be retained solely by your legal or compliance department and shall not be made available at any point thereafter to personnel in

NON-DISCLOSURE AND CONFIDENTIALITY AGREEMENT

other departments, other representatives, or any other person, without the express prior written consent of the NHDRA. Notwithstanding the return or destruction of any Confidential Information, Contractor shall continue to be bound by the confidentiality and other obligations hereunder.

6. Nature of Obligations.

This Agreement may be modified or waived only by a separate writing executed by the parties hereto that expressly modifies or waives a term or condition. The Contractor's failure to comply with any of the terms hereof, including but not limited to Contractor's responsibility to ensure that its employees and representatives also abide by this Agreement shall constitute an event of default under the terms of the Contract.

7. Required Disclosure.

If Contractor becomes required (by deposition, interrogatory, request for documents, subpoena, civil investigative demand, regulatory review, or similar process) to disclose any of the Confidential Information, Contractor shall provide the NHDRA with prompt prior written notice of, and the terms of and circumstances surrounding, such requirement, to the extent permitted by applicable law, rule, or regulation, so that the NHDRA as intended third party beneficiary may seek a protective order or other appropriate remedy, and/or waive compliance with the terms and conditions of this Agreement. If such protective order or other remedy is not obtained, or if the NHDRA waives compliance with the provisions hereof, then Contractor shall disclose only that portion of the Confidential Information that, as advised by counsel, is reasonably necessary to ensure compliance with such requirement. In addition, Contractor shall not oppose any action, and shall, if not prohibited by law, cooperate with, assist, and join with the NHDRA, to seek an appropriate protective order or other reliable assurance to safeguard the Confidential Information.

8. Term.

The terms and conditions of this Agreement, and all obligations of confidentiality contained herein, shall remain in full force and effect indefinitely and without expiration. This Agreement shall be enforceable by the NHDRA against any assignee or successor of the Contractor, whether such transfer of the Contract and/or the Confidential Information was the result of an affirmative action taken by the Contractor or, as a matter of law, as in the case of the institution of a receivership under state law or in the filing of a petition for relief under the United States Bankruptcy Code.

9. Remedies and Waiver.

It is further understood and agreed that money damages may not be a sufficient remedy for any actual or threatened breach of any of the provisions of this Agreement, and that the NHDRA may seek specific performance, injunctive and other equitable relief as a remedy for any such actual or threatened breach, which breach by itself shall constitute irreparable harm. It is further understood and agreed that no failure or delay by the parties hereto in exercising any right, power, or

NON-DISCLOSURE AND CONFIDENTIALITY AGREEMENT

privilege hereunder shall operate as a waiver thereof, nor shall any single or partial exercise thereof preclude any other or further exercise thereof or the exercise of any other right, power, or privilege hereunder. In the event of any litigation relating to this Agreement, if a court of competent jurisdiction determines in a final non-appealable decision that this Agreement has been breached by any party (including a breach hereof by Contractor), then the non-prevailing party shall reimburse the prevailing party for any reasonable legal fees and expenses incurred in connection with all such litigation. The existence of any claim or cause of action that Contractor may have against the NHDRA shall not constitute a defense or bar to the enforcement of this Agreement.

10. Governing Law.

This Agreement shall be governed by and construed in accordance with the laws of the State of New Hampshire. The parties hereto irrevocably and unconditionally consent hereby to submit to the exclusive jurisdiction of the Superior Court of the State of New Hampshire in Merrimack County, for any action, suit, or proceeding arising out of or relating to this Agreement, and hereby further irrevocably and unconditionally waive and agree not to plead in such court that any such action, suit, or proceeding brought in any such court has been brought in an inconvenient forum.

11. Severability.

If any of the provisions of this Agreement is found to violate any statute, regulation, rule, order, or decree of any governmental authority, court, agency, or exchange, such invalidity shall not be deemed to affect any other provision hereof or the validity of the remainder of this Agreement, and such invalid provision shall be deemed deleted herefrom to the minimum extent necessary to cure such violation.

12. Assignment.

This Agreement shall be for the benefit of and shall be enforceable by the NHDRA, and its respective affiliates, successors, and assigns. It is understood that any assignment of the Contract by Contractor without the express prior written consent of the NHDRA shall be void and of no effect. It is further understood, however, that should the Contractor assign the Contract through affirmative assignment, merger or acquisition with or without the NHDRA's prior approval, or as a matter of law, as in the case of the institution of a receivership under state law or in the filing of a petition for relief under the United States Bankruptcy Code, this Agreement shall be enforceable by the NHDRA against the assignee or successor of the Contractor, as the case may be.

13. Counterparts.

This Agreement may be executed in one or more counterparts, and by the parties hereto on separate counterparts, each of which shall be deemed an original for all purposes and all of which together shall be deemed one and the same Agreement. A signed copy of this Agreement

NON-DISCLOSURE AND CONFIDENTIALITY AGREEMENT

delivered by facsimile, e-mail, PDF, or other means of electronic transmission shall be deemed to have the same legal effect as delivery of an original signed copy of this Agreement.

If you are in agreement with the foregoing, please sign and return the duplicate copy of this Agreement, which shall constitute the parties' entire agreement with respect to the subject matter hereof.

STATE OF NEW HAMPSHIRE
DEPARTMENT OF REVENUE ADMINISTRATION

By: _____

Name:

Title:

Date: _____, 20__.

[CONTRACTOR]

By: _____

Name:

Title:

Date: _____, 20__.

Department of Revenue Administration



POLICY and PROCEDURE

No. 22-001 Issue Date: 2/7/2022

Distribution: All Department Employees

Subject: Disclosures of Taxpayer and Department Information

NOTE: This Policy and Procedure is intended for the internal and disciplinary use of the Department of Revenue Administration and is not intended to establish any higher standard of care in any civil or criminal court proceeding or action than is otherwise provided by applicable state or federal law.

I. Purpose

The purpose of this Policy and Procedure is to set forth the policy for unauthorized disclosures of taxpayer and Department of Revenue Administration ("Department" or "DRA") information, including Federal Tax Information, the procedure for reporting such disclosures, and the disciplinary actions for such disclosures, for Department employees and contractors.

This Policy on Disclosures of Taxpayer and Department Information ("Policy") shall be read in a manner that is consistent with state and federal law, including, without limitation, RSA 21-J:14, Internal Revenue Code sections 7213 and 7213A, the associated Treasury Regulations, IRS Publication 1075, and all state administrative rules governing both the confidentiality of taxpayer information and employee discipline, as well as all relevant contracts, including contracts for the exchange of information with the federal government and other states, and the Collective Bargaining Agreement governing Executive Branch employees. In instances where this Policy conflicts with the aforementioned authorities, those authorities shall govern.

This Policy shall apply equally to all Department employees whether classified or unclassified.

This policy rescinds and replaces Policy # 14-018 "Disclosures of Taxpayer and Department Information, # 15-001 "Unauthorized Disclosures of Federal Tax Information," and #16-007 "Contractor Disclosures of Taxpayer and Department Information."

II. Definitions

For purposes of this Policy and Procedure, the term:

- A.** "Contractor" shall mean any individual or organization, including employees and subcontractors of such individuals or organizations, that the DRA contracts with for the provision of goods or services that has or may have access to any DRA information, including taxpayer records, files, returns, or return information. The term shall include any employee of a temporary employment or staffing agency assigned to work at the DRA.
- B.** "Disclosure Officer" shall mean the person designated by the Department to ensure compliance with the Department's safeguard standards and procedures as described in "Coordinating Safeguards within an Agency" of Pub 1075, and shall include for purposes hereof the "Alternate Disclosure Officer."
- C.** "Employee" shall mean an employee of the State of New Hampshire performing work at, or on behalf of, the DRA, including unpaid work or as an intern or volunteer.
- D.** "Federal Tax Information" or "FTI" shall mean any return or return information received from the Internal Revenue Service ("IRS") or secondary source, such as the Social Security Administration, Federal Office of Child Support Enforcement or Bureau of Fiscal Service. FTI includes any information created by the Department that is derived from return or return information including FTI presented in statistical format, unless aggregated in a manner that is permissible under Pub. 1075. FTI does not include federal tax returns or information provided directly to the Department by a taxpayer or their representative.

III. Policy

Taxpayer records, files, returns, or return information contained in the records of the Department, or developed by the Department or its contractors through their activities on its behalf, are confidential and privileged even in instances where identical information is public information in another individual's or organization's records. Employees and Contractors must only access and use confidential information for purposes allowed by law. A willful violation of RSA 21-J:14 constitutes a class A misdemeanor, punishable in accordance with RSA 626:2.

IRC § 7213(a)(2) makes the unauthorized disclosure of FTI by Employees and Contractors a potential felony offense. Additionally, IRC § 7213A makes the unauthorized inspection of FTI a misdemeanor, punishable by fines, imprisonment, or both. Finally, IRC § 7431 prescribes civil damages for unauthorized inspection or disclosure, and upon criminal indictment or

information under IRC § 7213 or § 7213A, requires notification to the taxpayer that an unauthorized inspection or disclosure has occurred.

Further, it is the responsibility of every DRA employee and contractor to read “Reporting Improper Inspections or Disclosures” of Pub 1075, found at <http://www.irs.gov/pub/irs-pdf/p1075.pdf> and to report any suspected unauthorized inspection or disclosure of FTI, including breaches and security incidents, as set forth below.

An impermissible disclosure includes, but is not limited to: (1) disclosing taxpayer information or DRA records or files to an individual or entity not authorized to receive it under RSA 21-J:14; (2) accessing taxpayer information or DRA records or files that exceeds what is necessary for the Employee to perform their job or the Contractor to perform the services the Contractor has been contracted to provide the DRA (each Contractor employee shall access only that information that is necessary to perform that individual employee’s job duties); (3) in the case of a Contractor, comingling taxpayer information or DRA records or files with any other files or records of the Contractor; (4) misusing, abusing, losing, or damaging the DRA’s records or information, including the failure to safeguard records, files, returns, or return information, or DRA information found in Contractor records; (5) publication of taxpayer information or DRA records or files in any public forum, including social media, networking or other public websites; and (6) in the case of FTI, any other disclosure that is impermissible under Pub 1075, IRC sections 6103, 7213 or 7213A, the associated Treasury regulations, or any other federal law or associated guidance.

It is the policy of the DRA that impermissible disclosures of taxpayer or Department information must be reported in accordance with the procedures below. In addition, it is the policy of the DRA that disciplinary action resulting from an impermissible disclosure of taxpayer or DRA information, shall be administered in accordance with the procedures below. Finally, it is the policy of the DRA that all contracts with DRA Contractors include provisions addressing the Contractor’s obligations with respect to taxpayer and DRA information as outlined below. Each Employee and Contractor shall annually attest that they have received, read, and understand this Policy.

IV. Procedures

A. PROTECTING FTI

All taxpayer information is confidential, and shall not be disclosed to other persons, except as authorized by power of attorney and in accordance with applicable law. However, FTI is subject to stricter confidentiality protections than other Department information. All Employees and Contractors are responsible for protecting FTI, regardless of whether such FTI is accessed through RIMS, the IRS electronic file transfer protocol (also known as the Secure Data Transfer application), the IRS website (including the Transcript Delivery System), hardcopies from IRS, or any other delivery method. Paper and electronic media containing FTI shall be strictly protected, monitored and controlled. Employees and Contractors shall comply with all internal DRA guidance and training concerning the protection of FTI. Generally, Employees and Contractors shall not print or photocopy FTI, except as expressly permitted by internal DRA written guidance. Further, Employees and Contractors shall not save or store FTI in electronic form on any DRA network, on or off premises, except as expressly permitted by internal DRA written guidance. Likewise, Employees and Contractors shall not transmit FTI by email, fax, phone call, or collaborative computing devices, except as expressly permitted by internal DRA written guidance.

FTI stored on electronic media shall be strictly controlled, encrypted and password protected. Paper documents containing FTI shall be stored and secured in the fourth floor vault as detailed in internal DRA written guidance. Paper documents provided by IRS (generally in response to a request using IRS form 8796A) containing FTI shall be locked in secure cabinets in the fourth floor vault and only accessed upon approval of the applicable Division Director and Disclosure Officer.

B. REPORTING REQUIREMENTS FOR ALL DISCLOSURES

When an Employee or Contractor knows or suspects that an impermissible disclosure has occurred with respect to any Department information, regardless of whether FTI is involved, the following procedure shall govern:

1. The Employee shall immediately report the impermissible disclosure to his or her Division Director. In the case of a Contractor, such Contractor shall immediately report the impermissible disclosure to a DRA Employee, who shall in turn immediately report the same to their Division Director. Each Employee or Contractor described in this subparagraph (including a DRA

Employee only aware of the disclosure through the report of a Contractor) shall be considered a "Reporting Party."

2. The Division Director shall complete a Disclosure Notification Report ("DNR"), review the completed information with the Reporting Parties, and have a Reporting Party sign and date the DNR. The Division Director shall also sign the completed DNR.
3. The Division Director shall file the completed DNR with the Assistant Commissioner's Office by the next business day following the Reporting Party's report of the impermissible disclosure.
4. Reported alleged disclosures shall be treated with the utmost level of confidentiality by the DRA, so the Reporting Party's and/or the alleged offender's identity shall be considered confidential and privileged.

C. REPORTING REQUIREMENTS FOR DISCLOSURES OF FTI

In the event an Employee suspects that there has been an unauthorized disclosure of FTI in any format, the following additional steps, which incorporate the requirements of IRS Pub. 1075, must be taken:

1. The Reporting Party shall notify, via e-mail correspondence, the following DRA personnel of the suspected unauthorized disclosure of FTI: the Assistant Commissioner, the Internal Auditor, the Disclosure Officer, and the Reporting Party's Division Director. The subject line of the Reporting Party's e-mail notifying of the alleged disclosure shall state "Suspected Unauthorized Disclosure of FTI."
2. The Reporting Party, in conjunction with the Disclosure Officer, shall immediately, but no later than 24 hours, report the suspected disclosure of FTI to the appropriate Agent-in-Charge at the Treasury Inspector General for Tax Administration (TIGTA) by calling the local field division office (currently, New York), or, if unable to contact such office, the TIGTA Hotline Number below:

Hotline Number: During normal business hours: 1-800-366-4484

After regular business hours: 1-800-589-3718

**Treasury Inspector General for Tax Administration
Ben Franklin Station
P.O. Box 589
Washington, DC 20044-0589**

3. Concurrently with the above, the Disclosure Officer shall notify, via email correspondence, the IRS Office of Safeguards at:

SafeguardReports@irs.gov. The Disclosure Officer's notification to the Office of Safeguards must occur even if all information is not yet available. If a determination is made that there should be discipline or other legal consequences as a result of the disclosure, the Disclosure Officer shall make a second notification to the Office of Safeguards. In the email correspondence notifying the Office of Safeguards, the Disclosure Officer shall document the specifics of the incident known at the time, including but not limited to:

- a. Name of agency and agency Point of Contact for resolving data incident with contact information;
- b. Date and time of the incident;
- c. Date and time the incident was discovered;
- d. How the incident was discovered;
- e. Description of the incident and the data involved, including specific data elements, if known;
- f. Potential number of FTI records involved; if unknown, a range shall be provided;
- g. Address where the incident occurred;
- h. IT involved (e.g. laptop, server, mainframe); and
- i. Whether the agency will initiate adverse or disciplinary action against an employee for an unauthorized inspection or disclosure of return information in violation of DRA policies. Adverse or disciplinary actions should be interpreted to include, but are not limited to, admonishments and censures, letters of warning, suspensions, reduction of job responsibilities, job reassignments, reductions in pay or denials of increment, and terminations. Adverse or disciplinary actions should also be interpreted to include alternatives that provide for any variety of both punitive and non-punitive remedial measures. All such adverse or disciplinary actions will be administered in accordance with law, the N.H. Personnel Rules, the CBA, and applicable procedures.

FTI data shall not be included in the data incident report. The identity of the person suspected of making the unauthorized disclosure shall not be included in any data incident reports to the IRS or the Office of Safeguards. Reports must be sent by the Disclosure Officer electronically and encrypted via IRS-approved encryption techniques. The Disclosure Officer shall use "data incident report" in the subject line of the email.

4. Upon receiving the notification, the Reporting Party's Division Director, Assistant Commissioner, Internal Auditor, Reporting Parties, and Responsible Parties, shall follow the steps set forth above in Section III (B) and (D).

5. The Division Director, Assistant Commissioner, Internal Auditor, and all other parties shall make every effort to exclude FTI from the DNR, the Disclosure Investigation Report, and any other document produced as part of the reporting or investigations of the potential disclosure(s).
6. The Assistant Commissioner shall notify an impacted taxpayer in writing when the DRA proposes an administrative determination as to disciplinary or adverse action against an Employee arising from the Employee's unauthorized inspection or disclosure of the taxpayer's return or return information. The required notice must include the date of the unauthorized inspection or disclosure and the rights of the taxpayer under IRC § 7431. The Assistant Commissioner shall also report to IRS Safeguards when taxpayer notification letters are issued. Taxpayer notification letters shall not include the identity of the person suspected of making or determined to have made any unauthorized disclosures.
7. In consultation with the Disclosure Officer, the Assistant Commissioner shall undertake appropriate measures for the remediation of unauthorized inspection or disclosure of a taxpayer's return or return information as necessary.

D. INVESTIGATING REQUIREMENTS FOR ALL DISCLOSURES

When the Assistant Commissioner's Office receives a completed DNR, regardless of whether the potential disclosure involved Department information or FTI, the following procedure shall govern:

1. The Assistant Commissioner shall review the completed DNR. If the impermissible disclosure appears to be willful, involve theft or conversion, or the suspected commission of a crime, the Assistant Commissioner shall consult with Revenue Counsel before an investigation is requested. As part of such consultation, the Assistant Commissioner and Revenue Counsel may in their discretion coordinate to notify the appropriate local, state and/or federal law enforcement authorities.
2. The Assistant Commissioner may request that the Internal Auditor (hereinafter, "Internal Auditor" shall include a designee selected at the discretion of the Assistant Commissioner) conduct an investigation of the reported allegation to assist with determining if an offense has occurred. If an investigation is requested, the Assistant Commissioner shall provide the Internal Auditor with a copy of the completed DNR and keep the original completed DNR. If the Assistant Commissioner determines that an

investigation is unnecessary, the Assistant Commissioner shall proceed to Section IV(D)(11) (below).

3. After requesting that the Internal Auditor conduct an investigation, the Assistant Commissioner shall notify the Employee(s) or Contractor(s) believed to be responsible for the impermissible disclosure ("Responsible Party(ies)") in writing within 10 calendar days of receipt of the DNR that an investigation will be commenced and the reason(s) for the investigation.
4. The Internal Auditor shall interview the Reporting Parties, the Responsible Parties (if different than the Reporting Parties), and any other individuals believed to have information relating to the alleged impermissible disclosure. When interviewing any Reporting Party or Responsible Party that are DRA Employees, their Division Director(s) shall be present at the interview. In the case of Contractors, the supervisor(s) for the Reporting Party and Responsible Party may be present at the interview. Any Responsible Party or Reporting Party shall be entitled to have a union representative (if applicable) present at the interview upon request. Each interview shall be conducted separately and in accordance with the Division of Personnel administrative rules.
5. The Internal Auditor shall request:
 - i. Any and all documentation concerning the allegation;
 - ii. The names of all employees or other individuals that the Reporting Parties believe may have knowledge of the allegations; and
 - iii. Any further information that the Internal Auditor deems necessary.
6. The Internal Auditor shall conduct any further research and interviews necessary to investigate the allegation.
7. During an investigation, all Employees and Contractors shall cooperate in the investigation. Failure to cooperate in the investigation may result in termination of employment in the case of an Employee, and the DRA's exercise of any contractual or other legal remedies in the case of a Contractor.
8. During any investigation, the Assistant Commissioner shall provide the Responsible Parties with written notification of the status of the investigation and the probable date of completion of the investigation every 2 weeks.

9. At the close of an investigation, the Internal Auditor shall complete and sign a Disclosure Investigation Report ("DIR") and file the completed DIR with the Assistant Commissioner's office.
10. The Assistant Commissioner shall perform an analysis of the DNR and (if applicable) the DIR to determine whether an offense has been committed. If no offense has been committed, a "no offense" finding shall be issued. If an offense(s) has been committed, a finding of the offense(s) committed shall be issued. The Assistant Commissioner may request additional information from the Internal Auditor.
11. When the result of the analysis has been determined, the Assistant Commissioner shall meet with the Responsible Parties and shall provide written notice to the Responsible Parties of the Department's findings and conclusions, as well as the result of the investigation. The Responsible Party's Division Director shall attend this meeting. In the case of Contractors, the supervisor(s) for the Contractor Responsible Party may be present at this meeting.
12. If the analysis results in discipline, the Assistant Commissioner shall place copies of all documents pertaining to the disciplinary action in the Responsible Party's personnel file pursuant to Per 1501.03(b)(4) and 1501.04, redacted to eliminate any taxpayer information pursuant to 21-J:14. In the case of Contractors, the Assistant Commissioner may place copies of all documents pertaining to the disclosure in the DRA files relating to the Contractor, and shall consider whether any contractual or other legal remedies, including debarment pursuant to RSA 21-l: 11-c, are appropriate.
13. In the case of Employees, the Responsible Party shall have five (5) business days from the date written notice is received to request a meeting to refute the evidence and conclusions presented by the Assistant Commissioner. If the Responsible Party requests a meeting, a meeting shall be scheduled at a mutually convenient time but not later than five (5) business days from the date of the request. The Assistant Commissioner shall issue a decision after consideration of any additional information received during the meeting, in writing to the Responsible Party within five (5) business days of the requested meeting.
14. Any penalty determination shall be carried out in accordance with Per pt. 1002.

15. Should an employee dispute the disciplinary decision issued by the Assistant Commissioner and wish to invoke the Informal Settlement Procedures Outlined in Per pt. 205, appeal shall be directly to the Commissioner.

E. EMPLOYEE DISCIPLINARY ACTION FOR ALL DISCLOSURES

1. Disclosure of taxpayer information and taxpayer privacy violations.

Any violation under this section (intentional or otherwise) may result in discipline up to and including immediate dismissal, regardless of whether or not FTI was involved in the disclosure.

Offenses:

- a. Impermissible disclosure of taxpayer records, files, returns, or return information contained in the records of the Department, or developed by the Department through its activities, and any other protected and confidential taxpayer information.
- b. Exceeding authorized access to taxpayer records, files, returns, or return information contained in the records of the Department, or developed by the Department through its activities, and any other protected and confidential taxpayer information. Authorized access is limited to the access required for the employee to complete his or her job.

2. Misuse, abuse, loss, or damage to Department records or information. Any violation under this section (intentional or otherwise) may result in discipline up to and including immediate dismissal.

Offenses:

- a. Failure to safeguard the Department's records, files, returns, or return information contained in the records of the Department, or developed by the Department through its activities, and any other protected and confidential taxpayer information.
- b. A failure to safeguard arises when the Department's records, files, returns, or return information are carelessly, recklessly, negligently or intentionally lost or destroyed.

A failure to safeguard shall also include instances when the Department's records, files, returns or return information are available for inspection by those not authorized to see them or those without a business need to see them, regardless of whether anyone actually accesses the information, such as the failure to lock your computer, laptop, or other device when it is not in your immediate possession, leaving documents with sensitive

taxpayer information viewable on your desk when you are away from your desk, and leaving your office unlocked at the end of the day.

3. Failure to report violation or respond truthfully; bad faith reporting.

Any violation under this section may result in discipline up to and including immediate dismissal.

Offenses:

- a. Failure to report a known or suspected impermissible disclosure or other violation of this Policy.
- b. Failure to cooperate with an investigation undertaken under this Policy, including, but not limited to, any failure to answer fully and truthfully any interview questions.
- c. Making any false report of a disclosure with actual knowledge of such falsity, including falsely reporting a disclosure when the Reporting Party has actual knowledge that none occurred, or alleging that an innocent person committed an actual disclosure, when the Reporting Party has actual knowledge the disclosure was committed by another individual.

4. Key Factors In Determining Discipline. The absence or presence of the following factors may bear on the severity or duration of any sanction issued pursuant to this Policy.

- a. Failure to protect taxpayer records, files, returns, or return information contained in the records of the Department, or developed by the Department through its activities, and any other protected and confidential taxpayer information.
- b. Extent to which disclosure may compromise the Department's proprietary information or operations, or otherwise impacts the Department.
- c. Extent and type of information lost or destroyed, whether or not for personal gain.
- d. Extent of risk of identity theft.
- e. Failure to encrypt and/or protect passwords.
- f. Failure to cooperate in an investigation.
- g. Failure to report any known or suspected unauthorized disclosure.
- h. The number of previous violations of this Policy by the Responsible Party.
- i. Whether the violation was a willful, reckless or negligent act.

F. INCIDENT RESPONSE TESTING

1. Annually, the Disclosure Officer shall coordinate a test of the DRA's incident response capability by performing tabletop test exercises for Section IV(C). of this Policy and Procedure, using scenarios that include a data breach of FTI as such is described in Pub 1075.
2. The Disclosure Officer shall consult with the DoIT DRA Lead or other DRA employees responsible for maintaining consolidated data centers and off-site storage in the tabletop exercises.
3. Following each tabletop exercise, the Disclosure Officer shall produce a report to Revenue Counsel that shall address if the policy or procedures contained within should be updated or amended.

G. REQUIRED CONTRACT TERMS

Every contract entered into by the DRA with a Contractor shall contain contract terms substantially similar to those contained in "Confidential Information Contract Provisions" attached hereto as Exhibit A.

H. DISCLOSURE OFFICER

The Disclosure Officer, Alternate Disclosure Officer, and DoIT Helpdesk are incident response support resources, and may offer advice and assistance to users of the system for the handling and reporting of security and privacy incidents.

I. ANNUAL REVIEW

This Policy and Procedure shall be reviewed by Revenue Counsel annually and any required updates or amendments shall immediately be forwarded to the DRA Policy and Procedure Committee as set forth in DRA Policy #13-005, Policy and Procedure Committee.

APPROVED:



Lindsey M. Stepp, Commissioner

2/7/2022 _____
Date