

## INFORMATION SECURITY PLAN

### OBJECTIVE

This Informative Security Plan (the “Plan”) is intended to create effective administrative, technical and physical safeguards for the protection of personal information of employees who are residents of the Commonwealth of Massachusetts. The Plan sets forth **Gorman Tax Service’s** procedure for evaluating electronic and physical methods of accessing, collecting, storing, using, transmitting, and protecting personal information of residents of the Commonwealth of Massachusetts.

For purposes of this Plan, “personal information” means:

A Massachusetts resident’s first name and last name, or first initial and last name, in combination with any one or more of the following that relate to such resident:

- (a) Social Security number;
- (b) Driver’s license number or state-issued identification card number; or
- (c) Financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident’s financial account.

**Gorman Tax Service** recognizes that, in particular, it possesses the personal information of Massachusetts residents in the following places:

- Temporary hard copy client and prospective client files located in various desk drawers and filing cabinets throughout office area.
- Electronic customer files and tax returns located on one office server and eight computers and hard drives.
- Personnel files and benefits information for **Gorman Tax Service** employees located in file cabinets in Kris’ locked office.
- Payroll information for **Gorman Tax Service** employees, including direct deposit information located in filing cabinet in Kris’ locked office.

This Plan is intended to protect this information from unauthorized access and/or use.

### SCOPE

In formulating and implementing the Plan, we have: (1) indentified reasonably foreseeable internal and external risks to the security, confidentiality and/or integrity of any electronic, paper or other records containing personal information; (2) assessed the likelihood and potential danger of these threats, taking into consideration the sensitivity of the personal information; (3) evaluated the sufficiency of existing policies, procedures, customer information systems, and other safeguards in place to minimize those risks, (4) designed and implemented a plan that puts safeguards in place to minimize those risks, consistent with the requirements of 201 C.M.R. 17.00, and (5) plan to regularly monitor the effectiveness of those safeguards.

## **DATA SECURITY COORDINATOR**

The Company has designated Harry L. Gorman as the Data Security Coordinator to implement, supervise and maintain the Plan.

The Data Security Coordinator will be responsible for:

1. Initial implementation of the Plan;
2. Training employees;
3. Regular testing of the Plan's safeguards;
4. Evaluating the ability of service providers to comply with the law;
5. Reviewing the scope of the security measures in the Plan at least annually, or whenever there is a material change in business practices affecting the Plan;
6. Conducting an annual training session for all agency employees with access to personal information.

## **INTERNAL RISKS TO PERSONAL INFORMATION**

To combat internal risks to the security, confidentiality and/or integrity of records containing personal information, including any and all client files, the following measures will be taken:

1. Company employees should access customer files only for legitimate business purposes.
2. Only Kristine M. Gorman shall have access to personnel files, payroll information and employees' benefit information. Kris' office is under lock and key.
3. Files containing personal information should be maintained under lock and key when not in use. No employee is to transport any personal identification information outside of company premises. All personal information files shall be locked in preparer's office filing cabinet at end of work day.
4. When preparing tax returns in front of a client, no preparer is allowed to have any other files containing personal information of any other client on their desk, credenza, top of filing cabinet, or any other place in their office except in their filing cabinet. No secretary shall expose or have on their desk or any other area in the secretary area any files containing personal identification information. All files must be in the secretary desk file or secretary filing cabinet.
5. All employees shall not expose any personal identification information on their computers (name of person by itself not included) for another to see from any software program, email message or fax.
6. All employees must refrain from discussing clients name, phone numbers, social security numbers, bank information, PIN number, debit or credit card number, where another client may be within listening distance.

7. All employees, at pick up, must ask a client for their personal identification to ascertain they are the ones picking up their return. If someone else will be picking up the return the client's written permission is required. (A client's dependent return can be released to the parent if that parent has claimed the child on their return).
8. No employee shall transfer, copy, send, or fax any personal identification information to any personal computer or laptop not owned by Gorman Tax Service.
9. All employees shall remove all personal identification information out of their personal bins on a daily basis and lock it up in their office filing cabinet at the end of the work day.
10. When it is appropriate to destroy agency records, paper and electronic records containing personal information they must be destroyed in a manner in which personal information cannot be read or reconstructed. (Gorman Tax Service shreds all not used personal information at the end of the work day).
11. Shredding of all unused personal information worksheets, paper, copies of tax returns, etc. must be completed nightly.
12. Agency computers shall require a user ID password. Current employees' computer user IDs and passwords will be changed periodically. Electronic access to personal information shall be blocked after multiple unsuccessful attempts to log-in.
13. Terminated employees must: (1) return all records containing personal information, in any form (including all such information stored on laptops or other portable devices or media, and in files, records, work papers, etc.); (2) return all keys, IDs, access codes and/or badges; (3) be prohibited from accessing personal information; and (4) the terminated employee's access to e-mail, voicemail, agency internet and passwords will be invalidated.
14. Electronic access to personal information shall be restricted to active users and active user accounts only.
15. Employees are encouraged to report any suspicious or unauthorized use of customer information.
16. All security measures contained in this Plan shall be reviewed and reevaluated annually, or whenever there is a material change in the business.
17. Employees with access to personal information will be trained on this Plan.
18. Company employees who violate this Plan may be subject to discipline up to and including termination.
19. Gorman Tax Service maintains a *Secure File Transfer Web Portal* in which to send a clients tax return or other personal information which requires a password for access.

20. No employee is to email any personal information to anyone that would contain a Massachusetts resident's first name in combination with any one or more of the following data elements that relate to such resident: (a) *social security number*; (b) *driver's license number* or *state issued identification card*; or (c) *financial account number*, or *credit or debit card number*, with or without any required security code, access code, personal identification number or password, that would permit access to a resident's financial account.

The Company should ensure that vendors who are provided personal information have their own compliant written security plan.

## **EXTERNAL RISKS TO PERSONAL INFORMATION**

To minimize external risks to the security, integrity of records containing personal information, including any and all customer files, the following measures will be taken:

1. Visitors to the company shall not have access to records containing personal information.
2. The Company maintains up-to-date firewall protection and operating system security patches.
3. The Company maintains up-to-date versions of security software, which includes mal-ware protection with up-to-date patches and virus definitions.
4. Computer systems are monitored for unauthorized use.

## **IN THE EVENT A BREACH OF PERSONAL INFORMATION OCCURS**

A security breach occurs when there is an unauthorized acquisition or use of personal information of one or more Massachusetts residents. The following measures will be taken by the Company in the event of a security breach which creates a risk of identity theft to Massachusetts residents:

1. The Agency will notify the Office of Consumer Affairs and Business Regulations (OCABR) and the Attorney General's Office. This notice shall include the nature of the breach, the number of Massachusetts residents affected by the breach and all the steps the agency has taken to rectify the incident and to prevent any further breaches from occurring.
2. The Agency shall also notify the employee(s) or customer(s) affected by the breach. That notice shall include information concerning each resident's right to obtain a police report and how to request a security freeze on their consumer report, but shall not include information regarding the nature of the breach and the number of Massachusetts residents affected.