INFORMATION SECURITY PLAN

OBJECTIVE

This Information 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 the Agency'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;

The Agency recognizes that, in particular, it possesses the personal information of Massachusetts residents in the following places:

- hard copy customer and prospective customer files located in file cabinet
- electronic customer files located on desktop computer hard dri***ve***
- electronic customer or driver database located on desktop computer hard dri***ve***

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

SCOPE

In formulating and implementing the Plan, we have (1) identified 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 Agency has designated Tom DeVol as the Data Security Coordinator to implement, supervise and maintain the Plan.

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 customer files, such information should be maintained under lock and key when not being used. If such files need to be transported outside of the Agency, reasonable steps should be taken to maintain the security of the information. Agency computer(s) shall require a user log-in and password, and passwords will be changed periodically. Any employee who terminates his or her employment with the Agency should return all customer records and files, and that individual's access to Agency computers, e-mail or voice mail must be terminated.

.

The Agency 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 agency shall not have access to records containing personal information.

2. The Agency maintains up-to-date firewall protection and operating system security patches.

3. The Agency maintains up-to-date versions of security software, which includes mal-ware protection with up-to-date patches and virus definitions.

4. To the extent technically feasible, personal information stored on laptops or other portable devices in encrypted.

5. To the extent technically feasible, personal information transmitted across public networks or wirelessly is encrypted.

6. Computer systems are monitored for unauthorized use.

7. Secure user protocols are in place, including: (1) protocols for control of user IDs and other identifiers, (2) a secure method of assigning and selecting passwords, and (3) control of data security passwords to ensure that such passwords are kept in a location and/or format that does not compromise the security of the data they protect.

8. Employee log-ins and passwords are not vendor supplied default log-ins and passwords.

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 Agency 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 braches form 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.