LAPPIN FOUNDATION
WRITTEN INFORMATION SECURITY PLAN

1. Purpose and Scope. The Lappin Foundation (the "Organization") adopts this comprehensive written information security plan ("WISP"), developed in accordance with the requirements of the Massachusetts Data Security Regulation, 201 Code Mass. Regs. 17.01 to 17.05, for the purpose of documenting safeguards to protect personal information. This WISP applies to all employees, contractors, officers and directors of the Organization, and to any records that contain personal information in any format and on any media, whether electronic or paper form. For purposes of this WISP, "personal information" means either a Massachusetts resident's first and last name or first initial and last name in combination with any one or more of the following data elements, or any of the following data elements standing alone or in combination, if such data elements could be used to commit identity theft against the individual:

- **(i)** Social Security Number;
- **(ii)** Driver's license number, other government-issued identification number, including passport number, or tribal identification number; or
- **(iii)** 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 the individual's financial account.

Personal information does not include lawfully obtained information that is available to the general public, including publicly available information from federal, state or local governments.

2. Information Security Coordinator. The Organization shall designate an Information Security Coordinator (the "ISC") to maintain this WISP.

3. Identifying Risk. The ISC shall work with the management of the Organization to identify and assess reasonably foreseeable internal and external risks to the security of any electronic, paper or other records containing personal information, and to evaluate the effectiveness of the safeguards described in Section 4 hereunder.

4. Security Policies. The Organization's computer system, including any wireless system, shall, to the extent technically feasible, include the following security features:

- **(i)** secure user authentication protocols, including: (a) control of user IDs; (b) a reasonably secure method of assigning and selecting passwords; (c) 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; (d) restricting access to active users only; and (e) blocking access to user identification after multiple unsuccessful attempts to gain access to the computer or information technology system;

(ii) secure access control measures that: (a) restrict access to records and files containing personal information to those who need such information to perform their job duties; and (b) assign unique identifications plus passwords, which are not vendor supplied default passwords, to each person with computer access, that are reasonably designed to maintain the integrity of the security of the access controls;

(iii) encryption of: (a) all transmitted records and files containing personal information that will travel across public networks; (b) all data containing personal information to be transmitted wirelessly; and (c) all personal information stored on laptops or other portable devices;

(iv) reasonable monitoring of systems, for unauthorized use of or access to personal information;

(v) firewall protection and operating system security patches that are reasonably designed to maintain the integrity of personal information stored in the Organization's computer system;

(vi) reasonably up-to-date security software including malware protection; and

(vii) education and training of employees on the proper use of the computer security system and the importance of personal information security.

5. Disciplinary Measures. Violations of this WISP will result in disciplinary action, in accordance with the Organization's procedures and human resources policies.

6. Terminated Employee Access. The ISC shall work with the management of the Organization to ensure that terminated employees and/or contractors, immediately upon termination, do not have ongoing access to the Organization's information systems or records.

7. Third-Party Service Providers. The ISC shall work with the management of the Organization to oversee service providers by: (a) taking reasonable steps to select and retain third-party service providers that are capable of maintaining appropriate security measures, including those described in Section 4 hereunder, to protect personal information; and (b) requiring such providers by contract to implement and maintain such security measures.

8. Storage of Physical Records. The ISC shall work with the management of the Organization to ensure reasonable restrictions are placed upon physical access to records containing personal information by storing such records in locked facilities, storage areas or containers.

9. Regular Monitoring, Reviewing and Documenting. The ISC shall work with the management of the Organization to: (a) regularly monitor the WISP to ensure it is operating in a manner reasonably calculated to prevent unauthorized access to or unauthorized use of personal information; (b) review the scope of the security policies in Section 4 hereunder at least annually or whenever there is a material change in the Organization's practices that may reasonably implicate the security or integrity of records containing personal information; and (c) document responsive actions taken in connection with any incident involving a breach of security.