Exhibit 1
Agency Agreement

Information Security Requirements for Agencies

As part of the written information security program required by this Agreement, and in accordance with section 501.171, Florida Statutes, section 69O-128, Florida Administrative Code and other applicable law, Agency shall utilize security measures covering any of its information technology systems, including any wireless systems, that are used in any way for the purpose of transacting business with Citizens in accordance with this Agreement.

The security measures must be reasonable and must be appropriate to the activities being undertaken by the Agency and any of its Agency Personnel. Consistent with industry best practices and applicable law, the security measures shall, at a minimum, and to the extent technically feasible, have the following elements:

1. Secure user authentication protocols including:

   (a) control of user IDs and other identifiers;

   (b) a reasonably secure method of assigning and selecting passwords, or use of unique identifier technologies, such as biometrics or token devices;

   (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 and active user accounts only; and

   (e) blocking access to user identification after multiple unsuccessful authentication attempts;

2. Secure access control measures that:

   (a) restrict access to records and files containing Confidential 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;

3. Encryption of all transmitted records and files containing Confidential Information that will travel across public networks, and encryption of all data containing Confidential Information to be transmitted wirelessly.

4. Reasonable monitoring of systems, for unauthorized use of or access to Confidential Information;

5. Encryption of all Confidential Information stored on laptops or other portable devices;

6. For files containing Confidential Information on a system that is connected to the Internet, there must be reasonably up-to-date firewall protection and operating system security patches, reasonably designed to maintain the integrity of the Confidential Information.

7. Reasonably up-to-date versions of system security agent software which must include malware protection and reasonably up-to-date patches and virus definitions, or a version of such software that can still be supported with up-to-date patches and virus definitions, and is set to receive the most current security updates on a regular basis.