

# DATA SECURITY POLICIES AND PROCEDURES

**Winslow, EVANS & CROCKER, INC.  
Winslow, EVANS & CROCKER INSURANCE  
AGENCY, INC.**

**CRD No. 29686**

175 Federal St. 6<sup>th</sup> Floor  
Boston, MA 02110

These data security policies and procedures were approved by Leonid Berline – Executive Vice President, Chief Compliance Officer. These procedures are effective from the date approved until the date of their authorized revision, update or replacement.

Authorized Approval Signature: \_\_\_\_\_

Date these procedures became effective: March 1, 2010

Date these procedures were no longer effective (date of revision, update or replacement): \_\_\_\_\_

Recordkeeping: Discard after \_\_\_\_\_ (date three years from termination of use).

Adopted March 1, 2010

M.G.L. c. 93H was adopted by the legislature to protect the personal information of residents in the Commonwealth and the Office of Consumer Affairs and Business Regulation has adopted rules to implement the Act. Winslow, Evans & Crocker, Inc. and Winslow, Evans & Crocker Insurance Agency, Inc. (hereinafter collectively "Winslow") is required to comply with the rules with respect to Massachusetts' residents. The Rules impose a duty on every person that owns, licenses, stores or maintains Personal Information about a resident of the Commonwealth to develop, implement, maintain and monitor a comprehensive, written information security program.

### **Personal Information**

The rules define Personal Information as the name, either a first name or initial and a last name with any one or more of the following:

- (a) social Security number
- (b) driver's license or state issued ID number, or
- (c) financial account number, or credit or debit card number, with or without any required security code, access code, PIN or password, that would permit access to a resident's financial account.

### **Designated Security Program Officer**

Winslow has designated Leonid Berline, Chief Compliance Officer of Winslow, Evans & Crocker, Inc. as the Designated Security Program Officer ("DSPO"). The DSPO is charged with developing, implementing, maintaining and monitoring the system to ensure that the Firm meets the requirements to safeguard Personal Information in a manner reasonably designed, in light of the size, scope and type of business; the available resources; the amount of stored data; and the need for security and confidentiality of both consumer and employee information.

Winslow maintains Personal Information with respect to customers, employees and 1099 vendors who are residents of the Commonwealth.

### **Comprehensive Information Security Program**

#### 1.) Internal and External Risks

Winslow has reviewed the scope of Personal Information it maintains, stores or otherwise has access to or control over in connection with Winslow's client base, its employees and independent contractors who are residents of the Commonwealth. Such data includes:

##### Customers

- (i) Name, address, social security numbers and other identifying personal information

- (ii) Bank and other financial institution account numbers
- (iii) Employment

Employees and Independent Contractors

- (i) job applications and employment questionnaires
- (ii) I-9, W-2, W-4, K-1 and 1099 forms
- (iii) wage reporting and payroll withholding reports filed with federal and state agencies
- (iv) background checks
- (v) payroll processing information, and
- (vi) shareholder information

The risks involved with respect to Personal Information involve the unauthorized access to the Personal Information from within by employees whose job functions would not require such access; from third parties providing services to Winslow gaining access to Personal Information; from the theft of files, computers, laptops; tapping into data transmissions; and access to paper files or drives being discarded.

Winslow requires that all such Personal Information be maintained in physical files that are locked when not being used; that only authorized employees on a needs basis have access to the locked files; that files not be left unattended where unauthorized persons could obtain Personal Information; that Personal Information may not be stored on laptops; that offsite access to computer files be password restricted and only through encryption technology; that employees may not remove Personal Information from Winslow's premises; that third party vendors (payroll service providers and employment verification services for example) receive and transmit using encryption technology; and that all third party vendors certify that they are in compliance with M.G.L. c.93H.

2.) Disciplinary Policy

Winslow considers violations of its policies regarding Personal Information as a basis for imposing disciplinary action on the offending employee. The discipline can range from a warning to termination of employment depending upon the nature and severity of the breach.

3.) Employee Education and Training

Every employee has been provided with a copy of this policy and has acknowledged its receipt and his or her duty to read and comply with the policy. The DSPO is the person to whom employees can report breaches of the policies and from whom they may seek guidance regarding the program and its ongoing requirements.

#### 4.) Terminated Employees

When an employee's employment terminates, access to the premises is restricted, keys to secure areas are retrieved and password access to computer files is terminated. Employees taking property from the premises may only take their own personal property and may not take any files, computers or data belonging to Winslow. Terminated employees are asked to certify that they have no Personal Information in their control or possession.

#### 4.) Collected Personal Information

As a policy, Winslow only obtains the minimum Personal Information necessary to meet its obligations as a registered broker/dealer, investment adviser and as a licensed insurance agency and as an employer and only to meet its legitimate business needs. When Personal Information is no longer required to be kept under federal and state laws, rules and regulations, the DSPO will oversee the destruction of the Personal Information.

#### 5.) Annual Review

At least annually, the DSPO will have the policies and procedures reviewed and tested to ensure compliance. If the type of business engaged in were to change so that other sources of Personal Information were obtained, the DSPO will cause the policies and procedures to be amended to cover the additional data and file sources.

#### 6.) Breach of Security

In the event that a breach of security is discovered, the DSPO will immediately notify the resident(s) whose Personal Information has been compromised, the Attorney General and the Office of Consumer Affairs and Business Regulation.

### **Computer System Security Requirements**

Winslow's computer system, including wireless systems that contain Personal Information:

1.) have secure user authentication protocols including:

- (i) control of user ID's and other identifiers;
- (ii) a reasonable secure method of assigning and selecting passwords, or use of unique identifier technologies

- (iii) 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;
  - (iv) restrict access to active users and active user accounts only; and
  - (v) blocking access to user identification after multiple unsuccessful attempts to gain access
  
- 2.) Secure access control measures that:
  - (i) restrict access to records and files containing Personal Information to those who have a need to know; and
  - (ii) 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 access controls.
  
- 3.) Winslow requires encryption, to the extent technically feasible, of all transmitted records and files containing personal Information that will travel across public networks, and encryption of all data containing Personal Information to be transmitted wirelessly.
  
- 4.) Winslow's computer system monitors for unauthorized use of or access to Personal Information.
  
- 5.) Winslow prohibits the storage of Personal Information on laptop or other portable devices.
  
- 6.) Winslow has established up-to-date firewall security systems and security patches designed to maintain the integrity of the Personal Information.
  
- 7.) Winslow security agent software is maintained on a current basis and includes malware protection and reasonably up-to-date patches and virus definitions, and is set to receive security updates on a regular basis.
  
- 8.) Winslow requires employees be trained on the proper use of computer security systems and the importance of Personal Information.

**VENDOR CERTIFICATION**

\_\_\_\_\_, a vendor who creates, maintains, uses or transmits Personal Information, as defined in M.G.L. c. 93H, hereby certifies to Winslow Advisers Limited Partnership that it has complied with the law and 201 CMR 17:00 promulgated by the Office of Consumer Affairs and Business Regulation regarding the security of Personal information and hereby represents that Winslow Advisers limited Partnership may rely on this certification in meeting its obligation to protect Personal Information.

\_\_\_\_\_  
By: \_\_\_\_\_  
Its: \_\_\_\_\_  
Date: \_\_\_\_\_

**WINSLOW, EVANS & CROCKER, INC.**  
**DATA SECURITY**

The Commonwealth of Massachusetts enacted M.G.L. c 93H, a statute entitled Security Breaches, to provide for the safeguarding of personal information of residents of the Commonwealth. The Office of Consumer Affairs and Business Regulation is the state agency empowered to adopt regulations to implement the law. As part of those regulations, all businesses that have personal information regarding Massachusetts residents must adopt and enforce comprehensive written procedures designed to protect such information.

Winslow, Evans & Crocker, Inc. has adopted a comprehensive written policy with appropriate procedures to protect personal information that it receives in the course of its businesses as a broker/dealer and investment adviser.

# ACKNOWLEDGMENT

## ANNUAL CERTIFICATION OF COMPLIANCE WITH THE COMPANY'S DATA SECURITY POLICIES AND PROCEDURES

I certify that during the year ended as of the date written below:

I have read the above Winslow, Evans & Crocker, Inc. Data Security Policies and Procedures and agree to comply with the provisions contained therein.

---

Signature

---

Date

---

Name Printed