ELECTRONIC LOCKBOX SERVICES, LLC

Security Policy

Effective Date: **September 25, 2012**
Last Modified: **September 25, 2012**

1. Scope of Security Policy.
This Security Policy summarizes the principles, practices, and institutional controls that Electronic Lockbox Services, LLC ("ELS") has adopted to protect the security of your data.

2. Information Security Management.

(a) **Security Policy Document(s):** ELS maintains data security policy document(s) based on key controls and risk assessments.

(b) **Enforcement:** The Director of Information Technology is responsible for enforcement of this Security Policy.

(c) **Contact with Special Interest Groups:** ELS maintains appropriate contacts with selected groups and associations within the security community:

i. to facilitate ongoing security education and training for organizational ELS personnel;

ii. to stay up to date with the latest recommended security practices, techniques, and technologies; and

iii. to share current security-related information including threats, vulnerabilities, and incidents.

(d) **Independent Review of Data Security:** ELS will conduct an annual independent review of data risk management.

(e) **Management of Risks in Third Party Relationships:**

i. ELS will periodically review the risks from business processes involving external parties and implement appropriate controls against risks to the confidentiality and integrity of any data.

ii. ELS requires that providers of external information system services comply with organizational data security requirements and employ reasonable security controls in accordance with applicable laws, and ELS security and privacy policies.

(f) **Technical Compliance Checking:** ELS maintains and monitors technical controls.

(g) **Review of Access Rights:** ELS reviews users' access rights periodically.

(h) **Reporting of Information Security Incidents:** Information security events will be promptly reported.

(i) **Business Continuity Planning:** ELS maintains business continuity and disaster recovery plans.

3. **Information Asset Management**. ELS maintains company policies which specify requirements on acceptable use of electronic data. ELS classifies data based on sensitivity and corresponding risks; and maintains access control guidelines. ELS also provides data security awareness training to appropriate ELS personnel.

4. **Physical Security**.

(a) **Physical Security Controls:** Your data is housed in facilities with appropriate physical access controls, which may include barriers such as locks, alarms, walls, card-controlled entry gates or manned reception desks. Access to secured areas will be restricted to those with a legitimate business purpose.

(b) **Protection against Environmental Threats:** Your data is housed in facilities with appropriate protection from physical and environmental threats including but not limited to fire, flood, severe weather, explosion, theft, and other forms of natural or man-made disaster.

(c) **Decommissioning of Data:** Prior to disposing any storage media, ELS has all sensitive data and licensed software removed and sanitized.

(d) **Equipment Maintenance and Security:** Maintenance and repairs on information system and physical security components must be approved by the Director of Technology and will be conducted in accordance with manufacturer or vendor specifications and/or organizational requirements. Records of maintenance and repair will be maintained and periodically reviewed.

5. **Computer Systems & Operations Management**. ELS has effected standards and procedures for changes to and monitoring of IT infrastructure. ELS has also established **s**tandards and procedures for the separation of duties and areas of security responsibility:

(a) **Anti-virus and Malicious Code Protection:** Your data resides on servers protected with systems for the detection, prevention and recovery from malicious code.

(b) **Information Back-up and Recovery:** ELS has effected standards and procedures for the back-up and recovery of your data.

(c) **Network Controls:** ELS IT infrastructure and applications environments are adequately managed and controlled, in order to be protected from threats, and maintain the integrity, confidentiality and availability of your data:

i. *Firewall Policy.* All systems processing or housing your data are protected by firewalls.

ii. *Wireless and Internet Encryption Policy.* Processing or transmission of sensitive data on open or public networks, including email servers, takes place through an encrypted session e.g. SSL.

(d) **Data Handling:** ELS has implemented standards and procedures for the handling and storage of your data to protect it from unauthorized disclosure or misuse. All ELS applications and websites adhere to PCI Data Security Standards.

(e) **Access Control Standard:** All access to your data is based upon a "business need to know" basis. Access to our secure services and data is logged and our audit logs are reviewed regularly.

(f) **Computer User Registration and Management Standard:** ELS has established **s**tandards and procedures for granting and revoking access user accounts and access to data.

(g) **User Identification and Authentication:** Each user must have a unique identifier (user ID) for his or her personal use alone. ELS employs a secure authentication technique to substantiate the identity of each user such as strong passwords. Passwords and PINs are encrypted in storage and during transmission.

(h) **Segregation of Systems:** Information system management functionality such as security and change control functions are segregated from user functionality using network technical controls.

(i) **Cryptographic – Encryption Standard:** All sensitive information is encrypted using industry standard high-level encryption. We offer the use of a secure server. All supplied sensitive/credit information is transmitted via Secure Socket Layer (SSL) technology and then encrypted into our payment gateway provider's database. We prohibit the storage of card numbers, magnetic stripe data and security codes on any devices. After a transaction, your private information (credit cards, social security numbers, financials etc.) will not be stored on our servers.

(j) **Control of Technical Vulnerabilities:** ELS maintains a process for management of technical vulnerabilities of information systems.