INFORMATION SECURITY PLAN

Rev 1.1 04-10-2018

1. OBJECTIVE

The objective of BluB0X Security in the development and implementation of this comprehensive information security program ("ISP"), is to create effective administrative, technical and physical safeguards for the protection of personal information of our customers, employees, and to comply with our obligations under local and federal laws. The ISP sets forth our procedure for evaluating and addressing our electronic and physical methods of accessing, collecting, storing, using, transmitting, and protecting personal information.

For purposes of this ISP, "personal information" is as defined as: a person's first name and last name or first initial and last name in combination with any one or more of the following data elements 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; provided, however, that "personal information" shall not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public.

2. PURPOSE

The purpose of the ISP is to better: (a) ensure the security and confidentiality of personal information; (b) protect against any reasonably anticipated threats or hazards to the security or integrity of such information; and (c) protect against unauthorized access to or use of such information in a manner that creates a substantial risk of identity theft or fraud.

3. SCOPE

In formulating and implementing the ISP, BluB0X Security has addressed and incorporated the following protocols:

3.1. Identified reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information;

3.2. Assessed the likelihood and potential damage of these threats, taking into consideration the sensitivity of the personal information;

3.3. Evaluated the sufficiency of existing policies, procedures, customer information systems, and other safeguards in place to control risks;

3.4. Designed and implemented an ISP that puts safeguards in place to minimize those risks; and

3.5. Implemented regular monitoring of the effectiveness of those safeguards.

4. DATA SECURITY COORDINATOR

BluB0X Security has designated Sean Dyer to implement, supervise and maintain the ISP. This designated employee (the "Data Security Coordinator") will be responsible for the following:

4.1. Implementation of the ISP including all provisions outlined in Section VII: Daily Operational Protocol;

4.2. Training of all employees;

4.3. Regular testing of the ISP's safeguards;

4.4. Evaluating the ability of any of our third party service providers to implement and maintain appropriate security measures for the personal information to which we have permitted them access, and requiring such third party service providers by contract to implement and maintain appropriate security measures;

4.5. Reviewing the scope of the security measures in the ISP at least annually, or whenever there is a material change in our business practices that may implicate the security or integrity of records containing personal information;

4.6. Conducting an annual training session for all owners, managers, employees and independent contractors, including temporary and contract employees who have access to personal information on the elements of the ISP. All attendees at such training sessions are required to certify their attendance at the training, and their familiarity with our requirements for ensuring the protection of personal information.

5. INTERNAL RISK MITIGATION POLICIES

To guard against internal risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, the following measures are mandatory and are effective immediately:

5.1. We will only collect personal information of clients, customers or employees that is necessary to accomplish our legitimate business transactions or to comply with any and all federal, state or local regulations.

5.2. Access to records containing personal information shall be limited to those employees whose duties, relevant to their job description, have a legitimate need to access said records, and only for this legitimate job-related purpose.

5.3. Written and electronic records containing personal information shall be securely destroyed or deleted at the earliest opportunity consistent with business needs or legal retention requirements.

5.4. A copy of the ISP is to be distributed to each current employee and to each new employee on the beginning date of their employment. It shall be the employee's responsibility for acknowledging in writing, by signing the attached sheet, that he/she has received a copy of the ISP and will abide by its provisions. Employees are encouraged and invited to advise the ISP Data Security Coordinator of any activities or operations which appear to pose risks to the security of personal information. If the

Data Security Coordinator is him or herself involved with these risks, employees are encouraged and invited to advise any other manager or supervisor or business owner.

5.5. A training session for all current employees will be held on Monday, January 22, 2018 to detail the provisions of the ISP.

5.6. All employment contracts, where applicable, will be amended to require all employees to comply with the provisions of the ISP and to prohibit any nonconforming use of personal data as defined by the ISP

5.7. Terminated employees must return all records containing personal data, in any form, in their possession at the time of termination. This includes all data stored on any portable device and any device owned directly by the terminated employee

5.8. A terminated employee's physical and electronic access to records containing personal information shall be restricted at the time of termination. This shall include remote electronic access to personal records, voicemail, internet, and email access. All keys, keycards, access devices, badges, company IDs, business cards, and the like shall be surrendered at the time of termination.

5.9. Disciplinary action will be applicable to violations of the ISP, irrespective of whether personal data was actually accessed or used without authorization.

5.10. All security measures including the ISP shall be reviewed at least annually beginning January 1, 2018 to ensure that the policies contained in the ISP are adequate meet all applicable federal and state regulations.

5.11. Should our business practices change in a way that impacts the collection, storage, and/or transportation of records containing personal information the ISP will be reviewed to ensure that the policies contained in the ISP are adequate to meet all applicable federal and state regulations.

5.12. The Data Security Coordinator or his/her designee shall be responsible for all review and modifications of the ISP and shall fully consult and apprise management of all reviews including any recommendations for improves security arising from the review.

5.13. The Data Security Coordinator shall maintain a secured and confidential master list of all passwords, and keys. The list will identify which employee possess password, keycards, or other access devices and that only approved employee have been provided access credentials

5.14. The Data Security Coordinator or his/her designee shall ensure that access to personal information in restricted to approved and active user accounts.

5.15. Current employees' user ID's and passwords shall conform to accepted security standards.

5.16. Employees are required to report suspicious or unauthorized use of personal information to a supervisor or the Data Security Coordinator

5.17. Whenever there is an incident that requires notification, the Data Security Coordinator shall host a mandatory post-incident review of events and actions taken, if any, in order to determine how to alter security practices to better safeguard personal information

6. EXTERNAL RISK MITIGATION POLICIES

6.1. Firewall protection, operating system security patches, and all software products shall be reasonably up-to-date and installed on any computer that stores or processes personal information

6.2. Personal information shall not be removed from the business premises in electronic or written form absent legitimate business need and use of reasonable security measures, as described in this policy

6.3. All system security software including, anti-virus, anti-malware, and internet security shall be reasonably up-to-date and installed on any computer that stores or processes personal information.

6.4. There shall be secure user authentication protocols in place that:

- Control user ID and other identifiers;
- Assigns passwords in a manner that conforms to accepted security standards, or applies use of unique identifier technologies;
- Control passwords to ensure that password information is secure.

7. DAILY OPERATIONAL PROTOCOL

This section of our ISP outlines our daily efforts to minimize security risks to any computer system that processes or stores personal information, ensures that physical files containing personal information are reasonable secured and develops daily employee practices designed to minimize access and security risks to personal information of our clients and/or customers and employees.

The Daily Operational Protocol is effective January 1, 2018 and shall be reviewed and modified as deemed necessary at a meeting of the Data Security Coordinator and personnel responsible and/or authorized for the security of personal information. The review meeting shall take place on or before January 20, 2018. Any modifications to the Daily Operational Protocol shall be published in an updated version of the ISP. At the time of publication, a copy of the ISP shall be distributed to all current employees and to new hires on their date of employment.

7.1. Recordkeeping Protocol

7.1.1. We will only collect personal information of clients and customers and employees that is necessary to accomplish our legitimate business transactions or to comply with any and all federal and state and local laws. We currently have no requirements to collect Social Security numbers (other than for our own employees) and shall refuse to collect said information except where it is collected inadvertently by taking a photograph of a credential (driver's license or passport) and said credential contains the Social Security Number.

7.1.2. Within 30 days of the publication of the ISP or any update the Data Security Coordinator or his/her designee shall perform an audit of all relevant company records to determine which records contain personal information, assign those files to the appropriate category, and to redact, expunge or otherwise eliminate all unnecessary personal information in a manner consistent with the ISP

7.1.3. Any personal information stored shall be disposed of when no longer needed for business purposes or required by law for storage. Disposal methods must be consistent with those prescribed by the ISP

7.1.4. Every effort shall be made to avoid creating paper copies of digital information that contains personal information as laid out by the ISP.

7.1.5. Any paper files containing personal information of clients or employees shall be stored in a locked filing cabinet. Only department heads and the Data Security Coordinator will be assigned keys to filing cabinets and only those individuals are allowed access to the paper files. Individual files may be assigned to employees on an as-needed basis by the department supervisor.

7.1.6. All employees are prohibited from keeping unsecured paper files containing personal information in their work area when they are not present (e.g. lunch breaks).

7.1.7. At the end of the day, all files containing personal information are to be returned to the locked filing cabinet by department heads or the Data Security Coordinator.

7.1.8. Paper or electronically stored records containing personal information shall be disposed of in a manner that complies with BluB0X policy and as follows:

7.1.9. Paper documents containing personal information shall be either redacted, burned, pulverized or shredded so that personal data cannot practicably be read or reconstructed;

7.1.10. Electronic media and other non-paper media containing personal information shall be destroyed or erased so that personal information cannot practicably be read or reconstructed.

7.1.11. The following employees are authorized to access and assign to other employees files containing personal information:

Employee Name	*Department*
Sean Dyer	*Engineering*
Patrick de Cavaignac	*Operations*

7.1.12. Electronic records containing personal information shall not be stored or transported on any portable electronic device, sent or transmitted electronically

7.1.13. to any portable device, or sent or transported electronically to any computer, portable or not, without being encrypted. The only exception shall be where there is no reasonable risk of unauthorized access to the personal information or it is technologically not feasible to encrypt the data as and where transmitted.

7.1.14. If necessary for the functioning of individual departments, the department head, in consultation with the Data Security Coordinator, may develop

departmental rules that ensure reasonable restrictions upon access and handling of files containing personal information and must comply with all ISP standards. Departmental rules are to be published as an addendum to the

7.2. Access Control Protocol

7.2.1. All our computers shall restrict user access to those employees having an authorized and unique log-in ID

7.2.2. All computers that have been inactive for 20 or more minutes shall require relog-in

7.2.3. After 5 unsuccessful web-site log-in attempts by any user ID, that user ID will be blocked from accessing any computer or file stored on any computer until access privileges are reestablished by the Data Security Coordinator or his/her designee

7.2.4. Access to electronically stored records containing personal information shall be electronically limited to those employees having an authorized and unique login ID

7.2.5. Where practical, all visitors who are expected to access areas other than common retail space or are granted access to office space containing personal information should be required to sign-in with a Photo ID at a designated reception area where they will be assigned a visitor's ID or guest badge unless escorted at all times. Visitors are required to wear said visitor ID in a plainly visible location on their body, unless escorted at all times.

7.2.6. Where practical, all visitors are restricted from areas where files containing personal information are stored. Alternatively, visitors must be escorted or accompanied by an approved employee in any area where files containing personal information are stored

7.2.7. Cleaning personnel (or others on site after normal business hours and not also authorized to have access to personal information) are not to have access to areas where files containing personal information are stored

7.2.8. All computers with an internet connection or any computer that stores or processes personal information must have a reasonably up-to-date version of software providing virus, anti-spyware and anti-malware protection installed and active at all times.

7.3. Third Party Service Provider Protocol

Any service provider or individual that receives, stores, maintains, processes, or otherwise is permitted access to any file containing personal information ("Third Party Service Provider") shall be required to meet the following standards (Examples include third parties who provide off-site backup storage copies of all our electronic data; paper record copying or storage service providers; contractors or vendors working with our customers and having authorized access to our records):

7.3.1. Any contract with a Third Party Service Provider signed on or after January 1, 2018 shall require the Service Provider to implement security standards consistent with the ISP.

7.3.2. It shall be the responsibility of the Data Security Coordinator to obtain reasonable confirmation that any Third Party Service Provider is capable of meeting security standards consistent with the ISP.

7.3.3. Any existing contracts with Third Party Service shall be reviewed by the Data Security Coordinator. These Service Providers shall meet the security standards consistent with ISP by January 1, 2019 or other Service Providers will be selected, when feasible to do so.

8. Breach of Data Security Protocol

Should any employee know of a security breach at any of our facilities, or that any unencrypted personal information has been lost or stolen or accessed without authorization, or that encrypted personal information along with the access code or security key has been acquired by an unauthorized person or for an unauthorized purpose, the following protocol is to be followed:

8.1. Employees are to notify the Data Security Coordinator or department head in the event of a known or suspected security breach or unauthorized use of personal information.

8.2. The Data Security Coordinator shall be responsible for drafting a security breach notification to be provided to the affected party and all required local and federal law enforcement agencies. The security breach notification shall include the following:

8.2.1. A detailed description of the nature and circumstances of the security breach or unauthorized acquisition or use of personal information;

8.2.2. The number of persons affected at the time the notification is submitted;

8.2.3. The steps already taken relative to the incident;

8.2.4. Any steps intended to be taken relative to the incident subsequent to the filing of the notification; and

8.2.5. Information regarding whether law enforcement officials are engaged in investing the incident

END OF DOCUMENT

APPENDIX A – Record Retention Policy - *only for personnel who have direct access to SQL Server*