BluJay Solutions Information Security Exhibit

1. GENERAL

This Company Information Security Exhibit ("**Exhibit**") outlines the logical and physical security requirements that are generally applicable to Company's performance of services for, or provision of services or products to, Customer under the Agreement ("**Security Requirements**"). Unless otherwise stated in the Agreement, the terms of this Exhibit shall take precedence and prevail over any conflicting or inconsistent provisions set forth in the Agreement; provided, however, that any security controls specified in the Agreement shall take precedence and prevail over the provisions of this Exhibit where (i) the Agreement expressly states such; or (ii) the security controls specified in the Agreement exceed those set forth in this Exhibit.

2. DEFINITIONS

(i) "**Company Personnel**" means Company employees and contractors.

(ii) "**Confidential Customer Data**" means the data deemed "Confidential Information" under the Agreement and any Personally Identifiable Information, including but not limited to, Sensitive Personal Information.

(iii) "**Customer Data**" means any data transmitted by the Customer or its authorized users to the Company or accessed or acquired by the Company in connection with the provision of Services under the Agreement.

(iv) "**Customer Systems**" means the systems of the Customer, managed by Customer and accessed by Company in connection with the provision of Software and/or Services, including computer systems, software, and networks and the technology and data stored on or accessible through utilization of such systems, software, and networks.

(v) "**Data Misuse**" means the inappropriate or wrongful exercise of the right or privilege, such as right or privilege to access information, the wrongful disclosure of that information or the malicious or otherwise improper executive of a function or operation.

(vi) "**Industry Standard(s)**" means any of the following:

(A) Used or adopted by a substantial number of companies comparable in size, stature, function to the Company;

(B) Prescribed for use by an applicable nationally recognized standards body; or

(C) Assessed by a significant number of recognized experts in the field as acceptable and reasonable, except where a recent disclosure/public finding uncovers a significant flaw/vulnerability in such standard.

(vii) "**Loss**" means the loss of control over Confidential information, such that one or more actors may further disclose or conduct Data Misuse.

(viii) "**Privileged Users**" means any users who have enhanced authority to access and configure network systems, including but not limited to system administrators and "super users" who can provision, install, upgrade, or modify credentials, operating systems, source code, applications and other network systems.

(ix) "**Sensitive Personal Information"** means information that identifies or relates to an identifiable individual (i.e., a person who can be identified, directly or indirectly, including, by reference to an identification number, location data, an online identifier or to one or more factors specific to the person's physical, physiological, mental, economic, cultural or social identity) and such similar data regulated under applicable law.

3. POLICIES, AWARENESS AND TRAINING

(a) Company maintains, internally publishes and enforces documented security policies and standards addressing core information security concepts, including provisions that require assessments of various information security related risks, vulnerabilities, threats, and the management of those risks to meet these requirements and conform to all applicable data protection laws and regulations.

(b) Company maintains a comprehensive written information security program, updates and/or reviews such program, as necessary, on no less than an annual basis. Company helps to ensure such program (x) complies with applicable law and aligns to applicable Industry Standards, (y) includes appropriate administrative, logical, technical, and physical safeguards that comply with this Exhibit, and (z) is reasonably designed to achieve the following objectives:

(A) To help secure the confidentiality, integrity, and availability of Customer Data;

(B) To protect against any threats or hazards to the security and integrity or availability of Customer Systems; and

(C) To prevent unauthorized or accidental access, acquisition, destruction, loss, deletion, disclosure, or alteration or use of Customer Data or Customer Systems.

(c) One or more qualified Company employees are designated with responsibility to maintain the Company Information Security Program. The program is endorsed and approved by Company executive management to protect Confidential Customer Data against Loss or Data Misuse associated with Company's performance under the applicable contractual agreement with Customer.

(d) Where applicable law prevents compliance with Security Requirements or where applicable law sets forth more stringent requirements than those set forth in this Exhibit, Company will comply with applicable law.

(e) Upon request, Company will disclose to Customer any shared third-party hosting facilities that will hold Customer Data and Company will take reasonable measures to help ensure such third parties materially comply with the applicable terms of this Exhibit.

(f) Company provides training on a general range of information security topics, including, but not limited to phishing and social engineering, security fundamentals, and data protection to existing Company Personnel on an annual basis and to new Company Personnel upon hire. For Company Personnel who are considered Privileged Users, Company provides mandatory annual role-specific training in Company's security policies and standards.

4. ACCESS CONTROL

(a) Company will permit only those Company Personnel and third parties who are needed to perform services under the Agreement to access Customer Data or Customer Systems. Authorized Company Personnel and third parties will use Customer Data or Customer Systems only as necessary to perform their obligations under the Agreement and this Exhibit.

(b) Company applies the "Principle of Least Privilege (PLP)" for access to only such information relating to Customer operations as are necessary to perform a legitimate business function. Company employs a secure and reliable method for enforcing authorization controls to limit access consistent with PLP. Compliance with PLP requires a process which will promptly terminate access to Company Personnel and third parties who no longer require access to perform under an Agreement (e.g. a terminated or reassigned employee/contractor).

(c) Company has a documented process for controlling User IDs and other identifiers to help ensure they are unique among users and are not shared.

(d) Company will follow applicable law, applicable Industry Standard measures, and aging procedures to limit opportunities for compromise of password security and for authentication and authorization of users. Company will not use shared or generic identification credentials to access Customer Data or Customer Systems. Password procedures are in place to support the following:

(A) Passwords consist of a minimum of eight (8) characters and

(B) include at least one alpha character and one numeric and one special character.

(C) In addition, passwords expire every ninety (90) days or less

(D) and user IDs are deactivated after no more than ten (10) failed log-in attempts.

(e) Company verifies identification of users identify before any password resets and accounts remaining inactive for 90 days are disabled.

(f) Where feasible, if a session has been idle for more than fifteen (15) minutes, the user is required to re-enter the password and reactive the session.

(g) Company periodically reviews and revokes access rights of users.

(h) Company provides and revokes Company-managed identification credentials via documented technical and logical control procedures.

(i) Authentication to Company's network resources, platforms, devices, servers, workstations, applications and devices is not allowed with default passwords and, if available, role-based access controls are used.

(j) All access to Customer Data and Customer Systems, if applicable, will be via a secured connection between Company's service locations (including access through any of Company's cloud service providers) and Customer.

5. SECURE DATA PROTECTION

(a) Company stores Confidential Customer Data only on devices meeting these Security Requirements.

(b) Company uses Industry Standard measures, including encryption, for preventing interception of or access to Confidential Information transiting networks. Transit over the public internet and other externally accessible networks requires transport encryption.

(c) Confidential Information contained in paper form or unencrypted electronic media is stored in a controlled space (e.g., individual office with a door) with standard, after-business-hours locking; or in locked storage containers (e.g., locked drawer, cabinet).

(d) Use of Confidential Customer Data in a nonproduction (test or development) environment is permitted only if approved by Customer.

(e) Company maintains secure data disposal procedures, including but not limited to using secure erase commands, degaussing, and "crypto-shredding" when needed. Company's procedures follow Industry Standards.

(f) When physically transporting digital media containing Confidential Customer Data, that information is protected using storage encryption. If approved by Customer, transport using a qualified courier, with tracking and in a physically secure container. Physical transport of paper documents or other physical media containing Confidential Customer Data must be protected against casual observation of the information and sent using reliable means which includes tracking.

(g) If Confidential Customer Data is stored in or processed in a Company server or datacenter facility, those facilities will meet the facility controls set out in these Security Requirements.

(h) Company has an Encryption and Key Management Standard that defines acceptable cryptography standards for use across systems and environments. This standard exists to address issues and provide clarification related to encryption by identifying specific requirements that information resources must meet:

(A) Company encrypts Confidential Customer Data at rest, in transit, and in use via AES minimum 128-bit encryption and 1024-bit cipher key length.

(B) Prior to being backed up, all Customer Data will be encrypted or equivalently secured.

(C) Company will use Industry Standard encryption methods available when transferring Customer data over the Internet.

6. ENDPOINT & NETWORK SECURITY

(a) Company installs, configures, and maintains perimeter and network security controls to prevent unauthorized access to Customer Data and/or Customer Systems.

(b) Company maintains and configures endpoint security software on servers, desktops, laptops, mobile, and portable digital media devices. Endpoint protections may include encryption software, incident detection systems, incident prevention systems, anti-malware software, in accordance with Industry Standards. Company will help ensure such configurations generate alerts to Company and logs accessible by the Company.

(c) Company implements Industry Standard controls (both in frequency and nature) at appropriate points in the Company network to control the ingress and egress of communication and data to environments containing Confidential Customer Data.

(d) Company will not bypass or attempt to circumvent established Company security controls, including when accessing external networks to Customer's systems.

(e) Company implements and maintains security and hardening standards for network devices, including, but not limited to baseline configurations, patching, passwords, and access control.

(f) Company follows documented change management procedures.

(g) Company changes default server passwords prior to placing devices or systems into production.

(h) Company maintains electronic logs of access and events to help ensure confirmation of access and protection of data. Logs are protected from unauthorized access, modification, and accidental or deliberate destruction. Log reviews are conducted on a regular basis.

(i) Company reasonably protects workstations from intrusion by implementing automatic screen savers, locking devices, privacy screens, and/or similar controls.

7. APPLICATION MANAGEMENT

(a) Regardless of the development methodology, Company maintains a Software Development Life Cycle (SDLC) process that incorporates security coding practices (e.g. OWASP Top 10).

(b) Application development, test, and production activities are separated.

(c) Access and storage of application source code is limited to support the Principle of Least Privilege (PLP) and maintained in a dedicated system (source code repository). Application source code is maintained using version control.

(d) Application documentation is kept up to date, held in accessible form, and protected from loss or damage.

(e) Internal developed Software is tested, including regression testing, as applicable, prior to deployment.

8. RISK MANAGEMENT

(a) Company maintains a risk assessment program, which defines roles and responsibilities for performing risk assessment and responding to results. Company performs an annual risk assessment to verify the design of controls that protect business operations and information technology.

(b) Company maintains a risk assessment remediation plan, which includes the use of issue tracking to completion that measures remediation progress regularly against target dates. For risk acceptance, Company management will provide clear acknowledgement and a description of the risk. The risk acceptance includes a business justification.

9. OPERATIONS MANAGEMENT

(a) Company systems and devices involved in the performance of an agreement are maintained and configured securely in accordance with established baselines and standards. Company has implemented Industry Standard virus/malware detection software and has an upgrade cadence.

(b) Company applies security patches and system updates to Company-managed software and applications, appliances, and operating systems in a reasonable time frame based on the criticality of the vulnerability, availability of the patch, and sensitivity of the underlying data. Patches will be provided to Customer upon their availability with the following schedule defining the acceptable limits for testing and applying patches.

(i) Company conducts regular security vulnerability scans of Company systems and networks.

(ii) Annually, Company performs network penetration testing of external networks.

(iii) Company will identify, triage, document, and remediate vulnerabilities and threats to Customer Data and Customer Systems.

(iv) Company will apply security patches and system updates to Company-managed software and systems, appliances, and operating systems in a reasonable time frame based on the criticality of an identified vulnerability, availability of the patch, and sensitivity of the underlying data.

10. BUSINESS CONTINUITY AND DISASTER RECOVERY

(a) Company maintains a documented Business Continuity Program (BCP). Company will review its BCP plans at least annually.

11. SECURITY INCIDENT MANAGEMENT AND RESPONSE

(a) As part of its Information Security Program, Company maintains and annually updates a documented plan for security incident management and response in the event of an actual or suspected security compromise.

(b) The Company's security incident management and response plan contains documented formal procedures that comply with Industry Standards and applicable laws addressing investigation and response to security incidents, including without limitation, government mandated notifications in the event of privacy breaches.

(c) Company will reasonably cooperate with Customer in any investigations of possible fraudulent or unauthorized use of or access to Customer Data or Customer Systems by Company's employees or third parties.

(d) If Company discovers or is notified of a breach of security which results in unauthorized access, acquisition, disclosure, or use relating to any Customer Data or Customer Systems or any violation of these Security Requirements, Company will provide notification to Customer as soon as reasonably possible.

(e) The Data Processing Addendum describes other actions that will be taken by Company in the event of a security breach.

12. PHYSICAL SECURITY

Company utilizes the following physical security measures where Confidential Customer Data is stored or is accessible.

(a) Company will only allow authorized individuals with reasonable business needs to access Company facilities and areas within such where Confidential Customer Data is stored or accessible.

(b) Systems providing Facility Access Control are secured from tampering, circumvention or destruction, are maintained in functional order at all times and are updated or changed if they become compromised or ineffective.

(c) Facility Controls meet or exceed applicable Industry Standards to prevent and detect physical compromise.

(d) Company periodically reviews compliance with Facility Controls to help ensure alignment of compliance and Security Requirements.

13. RIGHT TO AUDIT

(a) No more than once per calendar year (annually), at Customer's request and expenses, Customer may reasonably audit Company's compliance with this Exhibit. Such audit will take place during normal business hours and days upon at least 30 business days prior written notice to Company. The audit may be held on-site at Company's facility or remote. No later than 2 weeks before commencement of the audit Company and Customer will mutually agree upon the scope and timeline for the audit.

(b) Company shall reasonably cooperate with Customer's audit by providing Customer with documentation demonstrating compliance with this Exhibit.

(c) Upon request, Company will discuss any audit findings with Customer and mutually agree with Customer on remediation activities and timelines, if applicable.

(d) Upon request, in lieu of an audit, Company will provide Customer with an annual security questionnaire (not to exceed one (1) request in any twelve (12) month period) responding to specific questions on Company's information security program, as applicable.

END OF EXHIBIT