Written Information Security Program ("WISP")

for

busHive, Inc. ("busHive")

Effective Date: May 27th 2022

1. Purpose:

This WISP supports busHive's efforts to protect Confidential Information, as that term is defined in Appendix A, from unauthorized acquisition, use, disclosure and/or modification through various policies and procedures that are made part of and organized under this WISP. busHive has developed and structured this WISP, and the policies and procedures of which it is comprised, by analyzing, among other things: (i) the scope and type of activities busHive engages in; (ii) the amount and type of Confidential Information that is stored by busHive; and (iii) the need for security and confidentiality of such Confidential Information.

2. Scope:

This WISP applies to all Confidential Information received, maintained, processed, stored or transmitted by or for busHive (whether in electronic or other form) and covers all individual busHive employees or other users that have access to Confidential Information.

3. Data Security Coordinator:

busHive designates Michael Hinckley, President and Chief Executive Officer, as its Data Security Coordinator under this WISP. It is the duty of the Data Security Coordinator to (either directly or through appropriate delegation):

- Maintain and, as needed, update, this WISP and its underlying policies and procedures;
- Oversee appropriate and regular training under this WISP, whether internal or outsourced;
- Regularly analyze the WISP's safeguards and ensure WISP compliance, including as appropriate through the risk management process set forth in busHive's Risk Assessment Policy;
- Evaluate the ability of third-party service providers to implement and maintain appropriate security measures to protect any Confidential Information to which they may have potential access, as further described in busHive's Third-Party Service Provider Security Policy;
- On a periodic basis, review the scope of the protective measures referenced in this WISP as set forth in the Review section below; and
- Periodically report to necessary internal stakeholders regarding the status and sufficiency of this WISP and busHive's safeguards protecting Confidential Information.

When necessary, busHive will designate a succeeding or temporary Data Security Coordinator so as to ensure, at all points in time, that there exists a Data Security Coordinator to fulfill the above roles.

4. Risk Assessment:

Pursuant to busHive's Risk Assessment Policy, busHive will regularly identify and assess reasonably foreseeable internal and external risks, threats and hazards to the security, confidentiality, and/or integrity of any electronic or paper records containing Confidential Information, and evaluate and improve, where necessary or otherwise appropriate, the effectiveness of current safeguards that limit such risks. To this end, busHive will conduct regular security assessments that: (i) identify reasonably foreseeable risks to Confidential Information, including network and software design, information processing, storage, transmission and disposal; (ii) assess the likelihood of, and potential damage that could result from, such risks; and (iii) evaluate the sufficiency of relevant policies, procedures, systems, and safeguards in place to control such risks.

To aid in its assessment of risk, and leveraging its relationship with Microsoft Azure partner Atmosera (or other appropriate support), busHive will also perform regular penetration testing and system scans, and employ automated intrusion detection and prevention systems.

5. Safeguards:

busHive employs reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of Confidential Information, which are designed to help busHive identify, protect against, detect, respond to and recover from potential security incidents. Such safeguards address appropriate controls covering the following topics:

- information classification;
- information handling;
- user access management;
- encryption;
- computer and network security;
- physical security;
- incident reporting and response;
- employee and third-party service provider access to and use of Confidential Information; and
- information systems development and maintenance.

Administrative Safeguards. busHive's administrative safeguards contemplate, among other things:

(i) the designation of an individual to coordinate its WISP;

(ii) a process to identify reasonably foreseeable internal and external risks to Confidential Information, and assess whether existing safeguards adequately address such risks;

(iii) training pertaining to, and oversight and regular review of, busHive's WISP and security safeguards;

(iv) selecting third-party service providers that are capable of maintaining appropriate safeguards, and requiring service providers to maintain safeguards by contract;

(v) adjusting the WISP in light of changes or new circumstances; and

(vi) appropriate disciplinary action for those who fail to comply with security policies and procedures.

Technical Safeguards. busHive's technical safeguards contemplate the use of, among other things:

(i) appropriate user authentication protocols, including, for example, the use of secure, unique accounts and passwords of appropriate length and complexity, restricting access to only active, legitimate users, blocking access after multiple unsuccessful attempts to gain access, and otherwise placing limitations on access rights through appropriate measures, such as multi-factor authentication for employee accounts;

(ii) appropriate access control measures, including, for example, restricting access to Confidential Information such that only those with a need to know in order to perform their duties consistent with busHive's operations access such Confidential Information, and limiting access to users on a personalized and role-based basis where feasible and appropriate;

(iii) appropriate encryption practices in relation to files and systems containing Confidential Information;

(iv) reasonable monitoring practices to prevent, detect and respond to unauthorized use of or access to Confidential Information, or other events adversely impacting Confidential Information;

(v) reasonably current firewall protection and software patch management for systems that contain Confidential Information; and

(vi) reasonably current anti-virus protection that is configured to receive updates on a regular basis.

Physical Safeguards. busHive's physical safeguards contemplate the use of, among other things:

(i) data minimization efforts to limit the amount and type of Confidential Information (both electronic and paper) within busHive's systems or otherwise under its control;

(ii) reasonable protection of areas where Confidential Information, or assets containing such Confidential Information, may be physically accessed;

(iii) reasonable procedures for the removal of Confidential Information from electronic media and devices (such as laptops) before such media or devices are made available for re-use;

(iv) reasonable measures to protect against unauthorized access to or use of Confidential Information during or after the collection, transportation and destruction or disposal of the information; and

(v) secure disposal or destruction of records containing Confidential Information within a reasonable period of time, and when it is no longer needed for a legitimate busHive purpose, consistent with busHive's applicable customer relationships and contractual requirements.

6. Review:

busHive will periodically review the scope of its security measures detailed in and contemplated under this WISP, including whenever there is a material change in its practices that may reasonably implicate the security, confidentiality or integrity of Confidential Information. In addition, busHive will periodically evaluate and adjust its security measures in light of any testing or monitoring efforts and any other circumstances that it knows or has reason to know may have a material impact on this WISP.

7. Incident Response:

Pursuant to its Incident Response Plan, busHive will identify and respond to any known or suspected incident involving a breach of security affecting Confidential Information, and will review events and actions taken in connection with any such incident in order to mitigate, to the extent practicable, known harmful effects and make appropriate changes in practices relating to protection of Confidential Information. According to the circumstances, documentation generated in connection with incident response efforts may be protected by the attorney-client privilege, the work product doctrine, the common interest or joint defense privilege, or any other privilege or doctrine protecting such documentation from use or disclosure. It is busHive policy in this regard to protect and not waive any such applicable privilege or doctrine.

8. Enforcement:

Any person in violation of this WISP or any policy or procedure it comprises may be denied access to Confidential Information and may be subject to appropriate disciplinary action, as determined by the Data Security Coordinator.

Appendix A

Confidential Information is defined as:

(1) All individually identifiable non-public personal information, including any of the following:

(a) Social Security Number;

(b) driver's license number or driver authorization card;

(c) state identification card number;

(d) federal identification card number;

(e) tribal identification number;

(f) passport number;

(g) alien registration number;

(h) military identification number;

(i) individual taxpayer identification number;

(j) tax or payroll information;

(k) credit card number, debit card number or financial account number whether or not it is combined with any security code, access code, PIN or password needed to access an account;

(l) PIN code used to permit usage of a financial transaction card;

(m) medical identification number;

(n) information related to medical history, mental or physical condition, diagnosis, treatment or evaluation by a healthcare professional, or the payment for the provision of healthcare;

(o) insurance policy number;

(p) health insurance policy, certificate or subscriber identification number, and any other unique identifier used by a health insurer to identify a person which would permit access to an individual's health information;

(q) unique biometric data, including fingerprints;

(r) digital signature; and

(s) a username, email address or other account holder identifying information, in combination with a security code, access code, password or security question and answer that would permit access to an online account.

(2) With respect to any student, all of the above information and any other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person to identify the student with reasonable certainty, including:

(a) the student's name;

(b) the name of the student's parent or other family members;

(c) the address of the student or student's family;

(d) a student identification number;

(e) the student's date of birth; and

(f) a student's mother's maiden name.

(3) All other non-public information which, because of its value, content, or nature, busHive desires to keep secure and confidential, including, without limitation, proprietary business or financial information.