

NEW YORK STATE MODEL DATA PRIVACY AGREEMENT FOR EDUCATIONAL AGENCIES

Saratoga Springs City School District

and

Bushive

This Data Privacy Agreement ("DPA") is by and between the Saratoga Springs City School District ("EA"), an Educational Agency, and Bushive ("Contractor"), collectively, the "Parties".

ARTICLE I: DEFINITIONS

As used in this DPA, the following terms shall have the following meanings:

- 1. Breach:** The unauthorized acquisition, access, use, or disclosure of Personally Identifiable Information in a manner not permitted by State and federal laws, rules and regulations, or in a manner which compromises its security or privacy, or by or to a person not authorized to acquire, access, use, or receive it, or a Breach of Contractor's security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personally Identifiable Information.
- 2. Commercial or Marketing Purpose:** means the sale, use or disclosure of Personally Identifiable Information for purposes of receiving remuneration, whether directly or indirectly; the sale, use or disclosure of Personally Identifiable Information for advertising purposes; or the sale, use or disclosure of Personally Identifiable Information to develop, improve or market products or services to students.
- 3. Disclose:** To permit access to, or the release, transfer, or other communication of personally identifiable information by any means, including oral, written or electronic, whether intended or unintended.
- 4. Education Record:** An education record as defined in the Family Educational Rights and Privacy Act and its implementing regulations, 20 U.S.C. 1232g and 34 C.F.R. Part 99, respectively.
- 5. Educational Agency:** As defined in Education Law 2-d, a school district, board of cooperative educational services, school, charter school, or the New York State Education Department.
- 6. Eligible Student:** A student who is eighteen years of age or older.
- 7. Encrypt or Encryption:** As defined in the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule at 45 CFR 164.304, means the use of an algorithmic process to transform Personally Identifiable Information into an unusable, unreadable, or indecipherable form in which there is a low probability of assigning meaning without use of a confidential process or key.

8. **NIST Cybersecurity Framework:** The U.S. Department of Commerce National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity Version 1.1.
9. **Parent:** A parent, legal guardian or person in parental relation to the Student.
10. **Personally Identifiable Information (PII):** Means personally identifiable information as defined in section 99.3 of Title 34 of the Code of Federal Regulations implementing the Family Educational Rights and Privacy Act, 20 U.S.C 1232g , and Teacher or Principal APPR Data, as defined below.
11. **Release:** Shall have the same meaning as Disclose.
12. **School:** Any public elementary or secondary school including a charter school, universal pre-kindergarten program authorized pursuant to Education Law § 3602-e, an approved provider of preschool special education, any other publicly funded pre-kindergarten program, a school serving children in a special act school district as defined in Education Law § 4001, an approved private school for the education of students with disabilities, a State-supported school subject to the provisions of Article 85 of the Education Law, or a State-operated school subject to the provisions of Articles 87 or 88 of the Education Law.
13. **Student:** Any person attending or seeking to enroll in an Educational Agency.
14. **Student Data:** Personally identifiable information as defined in section 99.3 of Title 34 of the Code of Federal Regulations implementing the Family Educational Rights and Privacy Act, 20 U.S.C 1232g.
15. **Subcontractor:** Contractor's non-employee agents, consultants and/or subcontractors engaged in the provision of services pursuant to the Service Agreement.
16. **Teacher or Principal APPR Data:** Personally Identifiable Information from the records of an Educational Agency relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of Education Law §§ 3012-c and 3012-d.

ARTICLE II: PRIVACY AND SECURITY OF PII

1. **Compliance with Law.**

In order for Contractor to provide certain services ("Services") to the EA pursuant to a contract dated **7/01/2023 – 6/30/2024** ("Service Agreement"); Contractor may receive PII regulated by several New York and federal laws and regulations, among them, the Family Educational Rights and Privacy Act ("FERPA") at 12 U.S.C. 1232g (34 CFR Part 99); Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. 6501-6502 (16 CFR Part 312); Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h (34 CFR Part 98); the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. 1400 et seq. (34 CFR Part 300); New York Education Law Section 2-d; and the Commissioner of Education's Regulations at 8 NYCRR Part 121. The Parties enter this DPA to address the requirements

of New York law. Contractor agrees to maintain the confidentiality and security of PII in accordance with applicable New York, federal and local laws, rules and regulations.

2. Authorized Use.

Contractor has no property or licensing rights or claims of ownership to PII, and Contractor must not use PII for any purpose other than to provide the Services set forth in the Service Agreement. Neither the Services provided nor the manner in which such Services are provided shall violate New York law.

3. Data Security and Privacy Plan.

Contractor shall adopt and maintain administrative, technical and physical safeguards, measures and controls to manage privacy and security risks and protect PII in a manner that complies with New York State, federal and local laws and regulations and the EA's policies. Education Law Section 2-d requires that Contractor provide the EA with a Data Privacy and Security Plan that outlines such safeguards, measures and controls including how the Contractor will implement all applicable state, federal and local data security and privacy requirements. Contractor's Data Security and Privacy Plan is attached to this DPA as Exhibit C.

4. EA's Data Security and Privacy Policy

State law and regulation requires the EA to adopt a data security and privacy policy that complies with Part 121 of the Regulations of the Commissioner of Education and aligns with the NIST Cyber Security Framework. Contractor shall comply with the EA's data security and privacy policy and other applicable policies.

5. Right of Review and Audit.

Upon request by the EA, Contractor shall provide the EA with copies of its policies and related procedures that pertain to the protection of PII. It may be made available in a form that does not violate Contractor's own information security policies, confidentiality obligations, and applicable laws. In addition, Contractor may be required to undergo an audit of its privacy and security safeguards, measures and controls as it pertains to alignment with the requirements of New York State laws and regulations, the EA's policies applicable to Contractor, and alignment with the NIST Cybersecurity Framework performed by an independent third party at Contractor's expense, and provide the audit report to the EA. Contractor may provide the EA with a recent industry standard independent audit report on Contractor's privacy and security practices as an alternative to undergoing an audit.

6. Contractor's Employees and Subcontractors.

- (a) Contractor shall only disclose PII to Contractor's employees and subcontractors who need to know the PII in order to provide the Services and the disclosure of PII shall be limited to the extent necessary to provide such Services. Contractor shall ensure that all such employees and subcontractors comply with the terms of this DPA.
- (b) Contractor must ensure that each subcontractor performing functions pursuant to the Service Agreement where the subcontractor will receive or have access to PII is contractually bound by a written agreement that includes confidentiality and data security obligations equivalent to, consistent with, and no less protective than, those found in this DPA.
- (c) Contractor shall examine the data security and privacy measures of its subcontractors prior to utilizing the subcontractor. If at any point a subcontractor fails to materially comply with the requirements of this DPA, Contractor shall: notify the EA and remove such subcontractor's access to PII; and, as applicable, retrieve all PII received or stored by such subcontractor and/or ensure that PII has been securely deleted and destroyed in accordance with this DPA. In the event there is an incident in which the subcontractor compromises PII, Contractor shall follow the Data Breach reporting requirements set forth herein.
- (d) Contractor shall take full responsibility for the acts and omissions of its employees and subcontractors.
- (e) Contractor must not disclose PII to any other party unless such disclosure is required by statute, court order or subpoena, and the Contractor makes a reasonable effort to notify the EA of the court order or subpoena in advance of compliance but in any case, provides notice to the EA no later than the time the PII is disclosed, unless such disclosure to the EA is expressly prohibited by the statute, court order or subpoena.

7. Training.

Contractor shall ensure that all its employees and Subcontractors who have access to PII have received or will receive training on the federal and state laws governing confidentiality of such data prior to receiving access.

8. Termination

The obligations of this DPA shall continue and shall not terminate for as long as the Contractor or its sub-contractors retain PII or retain access to PII.

9. Data Return and Destruction of Data.

- (a) Protecting PII from unauthorized access and disclosure is of the utmost importance to the EA, and Contractor agrees that it is prohibited from retaining PII or continued access to PII or any copy, summary or extract of PII, on any storage medium (including, without limitation, in secure data centers and/or cloud-based facilities) whatsoever beyond the period of providing Services to the EA, unless such retention is either expressly authorized for a prescribed period by the Service Agreement or other written agreement between the Parties, or expressly requested by the EA for purposes of facilitating the transfer of PII to the EA or expressly required by law. As applicable, upon expiration or termination of the Service Agreement, Contractor shall transfer PII, in a format agreed to by the Parties to the EA.
- (b) If applicable, once the transfer of PII has been accomplished in accordance with the EA's written election to do so, Contractor agrees to return or destroy all PII when the purpose that necessitated its receipt by Contractor has been completed. Thereafter, with regard to all PII (including without limitation, all hard copies, archived copies, electronic versions, electronic imaging of hard copies) as well as any and all PII maintained on behalf of Contractor in a secure data center and/or cloud-based facilities that remain in the possession of Contractor or its Subcontractors, Contractor shall ensure that PII is securely deleted and/or destroyed in a manner that does not allow it to be retrieved or retrievable, read or reconstructed. Hard copy media must be shredded or destroyed such that PII cannot be read or otherwise reconstructed, and electronic media must be cleared, purged, or destroyed such that the PII cannot be retrieved. Only the destruction of paper PII, and not redaction, will satisfy the requirements for data destruction. Redaction is specifically excluded as a means of data destruction.
- (c) Contractor shall provide the EA with a written certification of the secure deletion and/or destruction of PII held by the Contractor or Subcontractors.
- (d) To the extent that Contractor and/or its subcontractors continue to be in possession of any de-identified data (i.e., data that has had all direct and indirect identifiers removed), they agree not to attempt to re-identify de-identified data and not to transfer de-identified data to any party.

10. Commercial or Marketing Use Prohibition.

Contractor agrees that it will not sell PII or use or disclose PII for a Commercial or Marketing Purpose.

11. Encryption.

Contractor shall use industry standard security measures including encryption protocols that comply with New York law and regulations to preserve and protect PII. Contractor must encrypt PII at rest and in transit in accordance with applicable New York laws and regulations.

12. Breach.

(a) Contractor shall promptly notify the EA of any Breach of PII without unreasonable delay no later than seven (7) business days after discovery of the Breach. Notifications required pursuant to this section must be in writing, given by personal delivery, e-mail transmission (if contact information is provided for the specific mode of delivery), or by registered or certified, and must to the extent available, include a description of the Breach which includes the date of the incident and the date of discovery; the types of PII affected and the number of records affected; a description of Contractor's investigation; and the contact information for representatives who can assist the EA. Notifications required by this section must be sent to the EA's District Superintendent or other head administrator with a copy to the Data Protection Office. Violations of the requirement to notify the EA shall be subject to a civil penalty pursuant to Education Law Section 2-d. The Breach of certain PII protected by Education Law Section 2-d may subject the Contractor to additional penalties.

(b) Notifications required under this paragraph must be provided to the EA at the following address:

David L'Hommedieu

Assistant Superintendent of Information Technology and Operational Innovation & Data Protection Officer

3 Blue Streak Blvd.

Saratoga Springs, NY 12866

D_lhommedieu@saratogaschools.org

13. Cooperation with Investigations.

Contractor agrees that it will cooperate with the EA and law enforcement, where necessary, in any investigations into a Breach. Any costs incidental to the required cooperation or participation of the Contractor or its' Authorized Users, as related to such investigations, will be the sole responsibility of the Contractor if such Breach is attributable to Contractor or its Subcontractors.

14. Notification to Individuals.

Where a Breach of PII occurs that is attributable to Contractor, Contractor shall pay for or promptly reimburse the EA for the full cost of the EA's notification to Parents, Eligible Students, teachers, and/or principals, in accordance with Education Law Section 2-d and 8 NYCRR Part 121.

15. Termination.

The confidentiality and data security obligations of the Contractor under this DPA shall survive any termination of this DPA but shall terminate upon Contractor's certifying that it has destroyed all PII.

ARTICLE III: PARENT AND ELIGIBLE STUDENT PROVISIONS

1. Parent and Eligible Student Access.

Education Law Section 2-d and FERPA provide Parents and Eligible Students the right to inspect and review their child's or the Eligible Student's Student Data stored or maintained by the EA. To the extent Student Data is held by Contractor pursuant to the Service Agreement, Contractor shall respond within thirty (30) calendar days to the EA's requests for access to Student Data so the EA can facilitate such review by a Parent or Eligible Student, and facilitate corrections, as necessary. If a Parent or Eligible Student contacts Contractor directly to review any of the Student Data held by Contractor pursuant to the Service Agreement, Contractor shall promptly notify the EA and refer the Parent or Eligible Student to the EA.

2. Bill of Rights for Data Privacy and Security.

As required by Education Law Section 2-d, the Parents Bill of Rights for Data Privacy and Security and the supplemental information for the Service Agreement are included as Exhibit A and Exhibit B, respectively, and incorporated into this DPA. Contractor shall complete and sign Exhibit B and append it to this DPA. Pursuant to Education Law Section 2-d, the EA is required to post the completed Exhibit B on its website.

ARTICLE IV: MISCELLANEOUS

1. Priority of Agreements and Precedence.

In the event of a conflict between and among the terms and conditions of this DPA, including all Exhibits attached hereto and incorporated herein and the Service Agreement, the terms and conditions of this DPA shall govern and prevail, shall survive the termination of the Service Agreement in the manner set forth herein, and shall supersede all prior communications, representations, or agreements, oral or written, by the Parties relating thereto.

2. Execution.

This DPA may be executed in one or more counterparts, all of which shall be considered one and the same document, as if all parties had executed a single original document, and may be executed utilizing an electronic signature and/ or electronic transmittal, and each signature thereto shall be and constitute an original signature, as if all parties had executed a single original document.

EDUCATIONAL AGENCY: Saratoga Springs CSD	CONTRACTOR: Bushive
BY: <i>[Signature]</i>	BY: <i>MICHAEL HINCKLEY</i>
<i>[Printed Name]</i> David L'Hommedieu	Michael Hinckley
<i>[Title]</i> Data Protection Officer	President
Date:	Date: October 18, 2023

EXHIBIT A - Education Law §2-d Bill of Rights for Data Privacy and Security

Parents (including legal guardians or persons in parental relationships) and Eligible Students (students 18 years and older) can expect the following:

1. A student's personally identifiable information (PII) cannot be sold or released for any Commercial or Marketing purpose. PII, as defined by Education Law § 2-d and the Family Educational Rights and Privacy Act ("FERPA"), includes direct identifiers such as a student's name or identification number, parent's name, or address; and indirect identifiers such as a student's date of birth, which when linked to or combined with other information can be used to distinguish or trace a student's identity. Please see FERPA's regulations at 34 CFR 99.3 for a more complete definition.
2. The right to inspect and review the complete contents of the student's education record stored or maintained by an educational agency. This right may not apply to Parents of an Eligible Student.
3. State and federal laws such as Education Law § 2-d; the Commissioner of Education's Regulations at 8 NYCRR Part 121, FERPA at 12 U.S.C. 1232g (34 CFR Part 99); Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. 6501-6502 (16 CFR Part 312); Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h (34 CFR Part 98); and the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. 1400 et seq. (34 CFR Part 300); protect the confidentiality of a student's identifiable information.
4. Safeguards associated with industry standards and best practices including, but not limited to, encryption, firewalls and password protection must be in place when student PII is stored or transferred.
5. A complete list of all student data elements collected by NYSED is available at www.nysed.gov/data-privacy-security/student-data-inventory and by writing to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234.
6. The right to have complaints about possible breaches and unauthorized disclosures of PII addressed. (i) Complaints should be submitted to the EA at sscsd_dpo@saratogaschools.org. (ii) Complaints may also be submitted to the NYS Education Department at www.nysed.gov/data-privacy-security/report-improper-disclosure, by mail to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234; by email to privacy@nysed.gov; or by telephone at 518-474-0937.
7. To be notified in accordance with applicable laws and regulations if a breach or unauthorized release of PII occurs.
8. Educational agency workers that handle PII will receive training on applicable state and federal laws, policies, and safeguards associated with industry standards and best practices that protect PII.
9. Educational agency contracts with vendors that receive PII will address statutory and regulatory data privacy and security requirements.

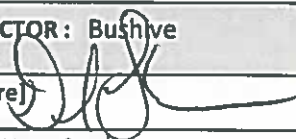
CONTRACTOR: Bushive	
[Signature]	
[Printed Name]	Michael Hinckley
[Title]	President
Date:	10-19-2023

EXHIBIT B

BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY - SUPPLEMENTAL INFORMATION FOR CONTRACTS THAT UTILIZE PERSONALLY IDENTIFIABLE INFORMATION

Pursuant to Education Law § 2-d and Section 121.3 of the Commissioner’s Regulations, the Educational Agency (EA) is required to post information to its website about its contracts with third-party contractors that will receive Personally Identifiable Information (PII).

Name of Contractor	Bushive
Description of the purpose(s) for which Contractor will receive/access PII	busHive provides technology to manage field trip requests, approvals and scheduling. It also manages driver compliance and vehicle preventative maintenance records.
Type of PII that Contractor will receive/access	Check all that apply: <input type="checkbox"/> Student PII <input checked="" type="checkbox"/> APPR Data
Contract Term	Contract Start Date <u>8/1/2023</u> Contract End Date <u>7/31/2024</u>
Subcontractor Written Agreement Requirement	Contractor will not utilize subcontractors without a written contract that requires the subcontractors to adhere to, at a minimum, materially similar data protection obligations imposed on the contractor by state and federal laws and regulations, and the Contract. (check applicable option) <input checked="" type="checkbox"/> Contractor will not utilize subcontractors. <input type="checkbox"/> Contractor will utilize subcontractors.
Data Transition and Secure Destruction	Upon expiration or termination of the Contract, Contractor shall: <ul style="list-style-type: none"> • Securely transfer data to EA, or a successor contractor at the EA’s option and written discretion, in a format agreed to by the parties. • Securely delete and destroy data.
Challenges to Data Accuracy	Parents, teachers or principals who seek to challenge the accuracy of PII will do so by contacting the EA. If a correction to data is deemed necessary, the EA will notify Contractor. Contractor agrees to facilitate such corrections within 21 days of receiving the EA’s written request.

Secure Storage and Data Security	<p>Please describe where PII will be stored and the protections taken to ensure PII will be protected: (check all that apply)</p> <p><input checked="" type="checkbox"/> Using a cloud or infrastructure owned and hosted by a third party.</p> <p><input type="checkbox"/> Using Contractor owned and hosted solution</p> <p><input type="checkbox"/> Other:</p> <p>Please describe how data security and privacy risks will be mitigated in a manner that does not compromise the security of the data:</p> <p>All busHive data is encrypted in SQL Azure using Transport Layer Security TLS (Encryption-in-transit) and further utilizes Transparent Data Encryption (Encryption-at-rest)</p>
Encryption	<p>Data will be encrypted while in motion and at rest.</p>

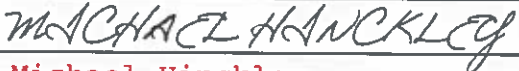
CONTRACTOR: Bushive	
[Signature]	
[Printed Name]	Michael Hinckley
[Title]	President
Date:	October 18, 2023

EXHIBIT C - CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

The Educational Agency (EA) is required to ensure that all contracts with a third-party contractor include a Data Security and Privacy Plan, pursuant to Education Law § 2-d and Section 121.6 of the Commissioner's Regulations. For every contract, the Contractor must complete the following or provide a plan that materially addresses its requirements, including alignment with the NIST Cybersecurity Framework, which is the standard for educational agency data privacy and security policies in New York state. **While this plan is not required to be posted to the EA's website, contractors should nevertheless ensure that they do not include information that could compromise the security of their data and data systems.**

1	Outline how you will implement applicable data security and privacy contract requirements over the life of the Contract.	See attached WISP, Security & Privacy Documents below
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	
3	Address the training received by your employees and any subcontractors engaged in the provision of services under the Contract on the federal and state laws that govern the confidentiality of PII.	
4	Outline contracting processes that ensure that your employees and any subcontractors are bound by written agreement to the requirements of the Contract, at a minimum.	
5	Specify how you will manage any data security and privacy incidents that implicate PII and describe any specific plans you have in place to identify breaches and/or unauthorized disclosures, and to meet your obligations to report incidents to the EA.	
6	Describe how data will be transitioned to the EA when no longer needed by you to meet your contractual obligations, if applicable.	
7	Describe your secure destruction practices and how certification will be provided to the EA.	
8	Outline how your data security and privacy program/practices align with the EA's applicable policies.	
9	Outline how your data security and privacy program/practices materially align with the NIST CSF v1.1 using the Framework chart below.	PLEASE USE TEMPLATE BELOW.

EXHIBIT C.1 – NIST CSF TABLE

The table below will aid the review of a Contractor's Data Privacy and Security Plan. Contractors should complete the Contractor Response sections in the table below to describe how their policies and practices align with each category in the Data Privacy and Security Plan template. To complete these 23 sections, a Contractor may: (i) Demonstrate alignment using the National Cybersecurity Review (NCSR) Maturity Scale of 1-7 ; (ii) Use a narrative to explain alignment (may reference its applicable policies); and/or (iii) Explain why a certain category may not apply to the transaction contemplated. Further informational references for each category can be found on the NIST website at <https://www.nist.gov/cyberframework/new-framework>. Please use additional pages if needed.

Function	Category	Contractor Response
IDENTIFY (ID)	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	See attached WISP, Security & Privacy Documents below
	Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	
	Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	
	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	
	Supply Chain Risk Management (ID.SC): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the	

Function	Category	Contractor Response
	processes to identify, assess and manage supply chain risks.	
PROTECT (PR)	Identity Management, Authentication and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	
	Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.	
	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	
	Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	
	Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	
DETECT (DE)	Anomalies and Events (DE.AE): Anomalous activity is detected and the potential impact of events is understood.	
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	

Function	Category	Contractor Response
RESPOND (RS)	Response Planning (RS.RP): Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.	
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	
	Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.	
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	
RECOVER (RC)	Recovery Planning (RC.RP): Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.	
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	
	Communications (RC.CO): Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).	



busHive[®]

TRANSPORTATION SOFTWARE

where all your operations come together

P.O. Box 417 / Ballston Spa, NY 12020 / 518.877.2500

[busHive.com](https://bushive.com)

busHive security, backup, and disaster recovery

All client data hosted by busHive is stored on Microsoft Azure Cloud. Microsoft spends over 1 Billion per year on cyber-security research and employs over 3500 security experts to oversee the security of their Azure cloud infrastructure. Furthermore, as of January 2020, they have more certifications than any other cloud provider. <https://azure.microsoft.com/en-us/overview/security/>

I. Backup and disaster recovery

<https://docs.microsoft.com/en-us/azure/sql-database/sql-database-automated-backups?tabs=single-database>

busHive hosts on 3 data centers with Microsoft: (Virginia, Wyoming and Toronto). Each client is regionally located in one server or the other, however continuous backups for 14 days are made using Azure [read-access geo-redundant storage \(RA-GRS\)](#) to ensure that they are preserved even if the data center is unavailable. We can thus restore to any Microsoft Data Center in the World.

SQL Database uses SQL Server technology to create [full backups](#) every week, [differential backups](#) every 24 hours, and [transaction log backups](#) every 5-10 minutes. The backups are stored in [RA-GRS storage blobs](#) that are replicated to a [paired data center](#) for protection against a data center outage. When you restore a database, the service figures out which full, differential, and transaction log backups need to be restored.

You can use these backups to:

- **Restore an existing database to a point-in-time in the past** within the retention period using the Azure portal, Azure PowerShell, Azure CLI, or REST API. In Single database and Elastic pools, this operation will create a new database in the same server as the original database. In Managed Instance, this operation can create a copy of the database or same or different Managed Instance under the same subscription.
- **Restore a deleted database to the time it was deleted** or anytime within the retention period. The deleted database can only be restored in the same logical server or Managed Instance where the original database was created.
- **Restore a database to another geographical region.** Geo-restore allows you to recover from a geographic disaster when you cannot access your server and database. It creates a new database in any existing server anywhere in the world.



busHive[®]

TRANSPORTATION SOFTWARE

where all your operations come together

P.O. Box 417 / Ballston Spa, NY 12020 / 518.877.2500

[busHive.com](https://bushive.com)

II. Encryption:

All busHive data is encrypted in SQL Azure using Transport Layer Security TLS (Encryption-in-transit) and further utilizes Transparent Data Encryption (Encryption-at-rest)

<https://docs.microsoft.com/en-us/azure/sql-database/sql-database-security-overview#transport-layer-security-tls-encryption-in-transit>

III. Microsoft Advanced data security (ADS)

busHive subscribes to Microsoft Advanced data security (ADS) for all servers hosting client data:

Advanced data security (ADS) provides a set of advanced SQL security capabilities, including data discovery & classification, vulnerability assessment, and Advanced Threat Protection.

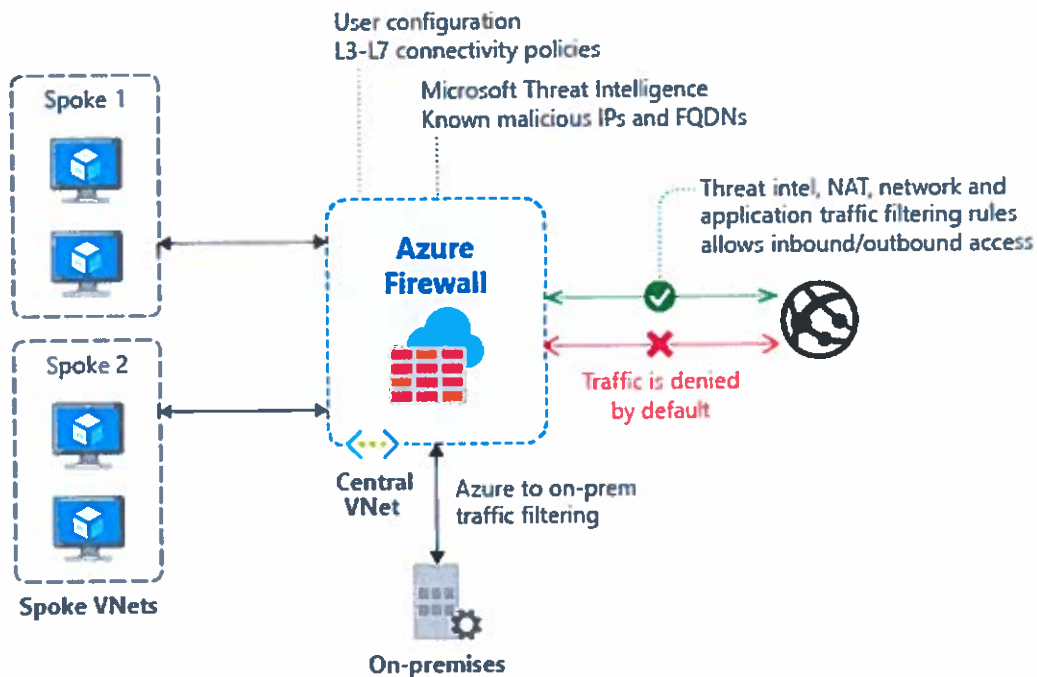
- [Vulnerability assessment](#) is an easy to configure service that can discover, track, and help remediate potential database vulnerabilities. It provides visibility into your security state, and includes actionable steps to resolve security issues, and enhance your database fortifications.
- [Advanced Threat Protection](#) detects anomalous activities indicating unusual and potentially harmful attempts to access or exploit your database. It continuously monitors your database for suspicious activities, and provides immediate security alerts on potential vulnerabilities, SQL injection attacks, and anomalous database access patterns. [Advanced Threat Protection alerts](#) provide details of the suspicious activity and recommend action on how to investigate and mitigate the threat.

<https://docs.microsoft.com/en-us/azure/sql-database/sql-database-advanced-data-security>

IV. Firewall

<https://docs.microsoft.com/en-us/azure/firewall/overview>

Azure Firewall is a managed, cloud-based network security service that protects your Azure Virtual Network resources. It's a fully stateful firewall as a service with built-in high availability and unrestricted cloud scalability.



busHive can centrally create, enforce, and log application and network connectivity policies across subscriptions and virtual networks. Azure Firewall uses a static public IP address for virtual network resources allowing outside firewalls to identify traffic originating from our virtual network. The service is fully integrated with Azure Monitor for logging and analytics.



TRANSPORTATION SOFTWARE

where all your operations come together

P.O. Box 417 / Ballston Spa, NY 12020 / 518.877.2500

busHive.com

V. No user passwords are stored in busHive databases.

busHive does not store user passwords in our databases with other user data. Instead, we have partnered with Microsoft Azure Active Directory B2C which allows us to have users authenticate via a secure outside source, which then passes us a token for access to busHive software. Storing user data without their passwords provides an important barrier to hackers seeking to retrieve user passwords for use on other sites.

<https://azure.microsoft.com/en-us/services/active-directory-b2c/>.

VI. Employee multi factor authentication

Finally, all busHive employees are required to authenticate using multi factor authentication.

VII. Cloud Inherent Risks

No human system is perfect. On May 3, 2019 Microsoft experienced a global outage of its network (<https://www.zdnet.com/article/azure-global-outage-our-dns-update-mangled-domain-records-says-microsoft/>) During this time for a few hours, our service was down and there was nothing that busHive could do but wait for it to come back online. No client data was lost that we know of, and as soon as the outage was resolved by Microsoft, the busHive application smoothly resumed functioning. For this reason, while busHive takes all reasonable steps to select a globally renowned cloud provider, and to maintain the highest levels of corporate security ourselves, we do not warrant uptime or security, as there are factors beyond our control that are the risks inherent to any application hosted on any cloud despite our best efforts to minimize that risk.

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.