RIDER

This is a Rider to the contract (including any terms of services or terms of use or any other policies, terms, agreements, or understandings referenced therein) between the Commack Union Free School District ("the District") and Goosechase Adventures Inc ("the Contractor"), that is being entered into for a Three year term for the use of Goosechase pursuant to the attached quote ("the Contract")(collectively, the Contract and Rider are referred to as "the Agreement").

To the extent that the provisions of this Rider and the annexed Data Privacy Agreement are inconsistent with any terms set forth in the Contract, the provisions of this Rider and the annexed Data Privacy Agreement will control.

1. Plan for Security and Protection of Personally Identifiable Information

   A. "District Data" means all information obtained by the Contractor from the District or by the Contractor in connection with the Services provided by the Contractor pursuant to this Agreement, including but not limited to business, administrative and financial data, intellectual property, student and personnel data, and metadata. The term, "District Data" does not include any information made publicly available by the District, except PII from student and personnel data which will be considered "District Data" regardless of whether or not it is made public.

   B. "Personally Identifiable Information" or "PII" includes, but is not limited to: (i) a person's name or address or the names or addresses of a student's parents or other family members; (ii) any personal identifier (e.g., SSN, student number or biometric record); (iii) indirect identifiers (e.g., date of birth, place of birth, or mother's maiden name); (iv) other information that alone or in combination is linked or linkable to a specific individual and would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances to identify the individual with reasonable certainty; and (v) any information requested by a person who the District or Contractor reasonably believes knows the identity of the person to whom a record relates.

   C. The Contractor represents and warrants that it will comply with all District policies and State, federal and local laws, regulations, rules and requirements related to the confidentiality, security and privacy of District Data.

   D. The Contractor represents and warrants that District Data received by the Contractor will be used only to perform Contractor's obligations pursuant to the Agreement and for no other purpose.

E. The Contractor represents and warrants that it will only collect data from the District or District employees or other End Users (the term "End Users" means the individuals authorized by the District to access and use services provided by the Contractor pursuant to the Agreement) that is necessary to fulfill the Contractor's duties pursuant to the Agreement.

F. The Parties agree that all rights including all intellectual property rights in and to District Data will remain the exclusive property of the District and that the Contractor has a limited, non-exclusive license to use District Data solely to perform the Services pursuant to the Agreement.

G. If the Contractor has access to District Data that is subject to the Family Educational Rights and Privacy Act ("FERPA"), the Contractor acknowledges that for purposes of the Agreement it will be designated as a "school official" with a "legitimate educational interest" pursuant to FERPA and its implementing regulations, and the Contractor agrees to abide by the limitations and requirements imposed on school officials.

H. The Contractor must execute and deliver the Data Privacy Agreement annexed hereto as Exhibit A simultaneously with the execution and delivery of this Rider. The terms of the Data Privacy Agreement are hereby incorporated into this Rider.

I. All the provisions of this Paragraph will survive the expiration or sooner termination of the Agreement.

2. Indemnification by the District: If the Contract has any provision that requires the District to indemnify, defend and/or hold harmless the Contractor, such provision will be void and have no force or effect.

3. Entire Agreement/No End User Agreements: The Agreement contains the entire agreement of the parties with respect to the subject matter thereof and supersedes any and all other agreements, understandings and representations, written or oral, by and between the parties. In the event that any part of the Agreement references terms of service or terms of use or any other policies, terms, agreements or understandings, the applicable policies, terms, agreements or understandings are those that were in effect on the date of the Contract, unless the applicable policies, terms, agreements or understandings were modified pursuant to Paragraph 6 of this Rider. In the event that the Consultant requires District employees or other End Users to enter into terms of use agreements or other agreements or understandings, whether electronic, click-through, verbal or in writing, those agreements and/or understandings will be null, void and without effect, and the terms of the Agreement will apply.

4. Termination: The Agreement may be terminated by the District immediately upon the Contractor's breach of the Contractor's obligations set forth in paragraph 1 of this Rider. Upon termination of the Agreement, the Contractor is not entitled to any further payments hereunder.

5. Notices: Any notices required or permitted to be given pursuant to the terms of the Agreement must be in writing and either personally delivered or sent by nationally recognized overnight carrier to the parties at the following addresses:

To the Contractor:

To the District:
Commack Union Free School District
PO Box 150
Commack, NY 11725
Attention: Superintendent of Schools

With a copy to:
Lamb & Barnosky, LLP
534 Broadhollow Road, Suite 210
P.O. Box 9034
Melville, New York 11747
Attention: Eugene R. Barnosky, Esq.

If the notice is sent by personal mail, it will be deemed delivered upon receipt and if sent by registered or certified mail, it shall be deemed delivered 3 days after so mailing.

6. Modification: The Agreement may not be changed by any District Employee or other End User. The Agreement may not be changed orally, electronically, by click-through agreement, or by continued use. The Agreement may only be changed by an agreement in writing signed by the District. Any waiver of any term, condition or provision of the Agreement will not constitute a waiver of any other term, condition or provision, nor will a waiver of any breach of any term, condition or provision constitute a waiver of any subsequent or succeeding breach.

7. Governing Law, Choice of Forum and Waiver of Jury Trial: The Agreement is subject to, governed by, enforced according to and construed according to the laws of the State of New York, without regard to the conflicts of laws provisions thereof. Notwithstanding the arbitration provisions in the Contract, if any, the parties agree that any dispute arising under the Agreement will be litigated in a New York State Court in Suffolk County, New York. The parties each waive trial by jury in any action concerning the Agreement.

8. No Assignment: In accordance with the provisions of New York General Municipal Law § 109, the Contractor is hereby prohibited from assigning, transferring, conveying, subletting or otherwise disposing of the Agreement, or of the Contractor's rights, title, or interest in the Agreement, or the Contractor's power to execute the Agreement to any other person or corporation without the previous consent in writing from the District.

9. Third-Party Beneficiaries: There are no third-party beneficiaries in the Agreement.

10. Execution: This Rider may be executed in one or more counterparts, all of which

shall be considered one and the same agreement. This Rider may be executed by facsimile or PDF signature, each of which shall constitute an original for all purposes.

11. Notwithstanding the execution of this Rider or any other term or condition of this Rider, it will not become effective unless and until the Contract between the parties is in full force and effect.

IN WITNESS WHEREOF, the parties hereto have duly executed this Agreement.

Commack Union Free School District

By: _____
Alise Pulliam
Executive Director for Instructional Technology

Type text here

Goosechase Adventures Inc., **the Contractor**

By: Stylianoudis
Name: Alexandre Stylianoudis
Title: Head of Legal and Finance

EXHIBIT A

DATA PRIVACY AGREEMENT

COMMACK UNION FREE SCHOOL DISTRICT
DATA PRIVACY AGREEMENT

Between

COMMACK UNION FREE SCHOOL DISTRICT

and

This Data Privacy Agreement ("DPA") is by and between the Commack Union Free School District ("the District") and Goosechase Adventures Inc. ("the Contractor"), collectively, "the Parties."

ARTICLE I: DEFINITIONS

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

1. Breach: The unauthorized acquisition, access, use, or disclosure of Personally Identifiable Information of District Data, or a breach of the 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: 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. District Data: All information obtained by the Contractor from the District or by the Contractor in connection with the Services provided by the Contractor pursuant to the Service Agreement, including but not limited to business, administrative and financial data, intellectual property, student and personnel data, and metadata. The term, "District Data" does not include any information made publicly available by the District, except Personally Identifiable Information from student and personnel data which will be considered "District Data" regardless of whether or not it is made public.

5. 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.

6. Educational Agency: As defined in Education Law 2-d, a school district, board of cooperative educational services, School, or the New York State Education Department.

7. Eligible Student: A student who is eighteen years of age or older.

8. 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.

9. NIST Cybersecurity Framework: The U.S. Department of Commerce National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity Version 1.1.

10. Parent: A parent, legal guardian or person in parental relation to the Student.

11. 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.

12. Release: Has the same meaning as Disclose.

13. Service Agreement:

The agreement between the District and the Contractor with an effective date of July 1, 2022.

14. Services: The services provided by the Contractor to the District pursuant to the Service Agreement.

15. 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.

16. Student: Any person attending or seeking to enroll in an Educational Agency.

17. 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. Personally Identifiable Information includes, but is not limited to: (i) a person's name or address or the names or addresses of a Student's parents or other family members; (ii) any personal identifier (*e.g.,* SSN, student number or biometric record); (iii) indirect identifiers (*e.g.,* date of birth, place of birth, or mother's maiden name); (iv) other information that alone or in combination is linked or linkable to a specific individual and would allow a reasonable person in the District community who does not have personal knowledge of the relevant circumstances to identify the individual with reasonable certainty; and (v) any information requested by a person who the District or the Contractor reasonably believes know the identity of the person to whom a record relates.

18. Subcontractor: The Contractor's non-employee agents, consultants and/or other persons or entities not employed by the Contractor who are engaged in the provision of Services pursuant to the Service Agreement.

19. 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 pursuant to the provisions of Education Law §§ 3012-c and 3012-d.

ARTICLE II: PRIVACY AND SECURITY OF PII

1. Compliance with Law.

In order for the Contractor to provide Services to the District pursuant to the Service Agreement; the Contractor may receive District Data regulated by several New York and federal laws and regulations, among them, the Family Educational Rights and Privacy Act ("FERPA") at 20 U.S.C. § 1232g (34 CFR Part 99); Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C.§§ 6501-6506 (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 § 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 and to protect District Data. The Contractor agrees to maintain the confidentiality and security of District Data in accordance with applicable New York, federal and local laws, rules and regulations.

2. Authorized Use.

The Contractor has no property or licensing rights or claims of ownership to District Data, and the Contractor must not use District Data for any purpose other than to provide the Services set forth in the Service Agreement. The Contractor agrees that neither the Services provided to the District nor the manner in which the Services are provided by the Contractor will violate applicable New York, federal and local laws, rules and regulations.

If the Contractor has access to District Data that is subject to the Family Educational Rights and Privacy Act ("FERPA"), the Contractor acknowledges that for purposes of this Agreement it will be designated as a "school official" with a "legitimate educational interest" pursuant to FERPA and its implementing regulations, and the Consultant agrees to abide by the limitations and requirements imposed on school officials.

3. Collection of Data.

The Contractor represents and warrants that it will only collect data from the District or District employees or other End Users (the term "End Users" means the individuals authorized by the District to access and use the Services) that is necessary to fulfill the Contractor's duties pursuant to the Service Agreement.

4. Data Security and Privacy Plan.

The Contractor must adopt and maintain administrative, technical and physical safeguards, measures and controls to manage privacy and security risks and protect District Data in a manner that complies with New York, federal and local laws, rules and regulations and the District's policies. Education Law § 2-d requires that the Contractor provide the District 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. The Contractor's Data Security and Privacy Plan is attached to this DPA as Exhibit C and is incorporated into this DPA.

5. The District's Data Security and Privacy Policy

State law and regulation requires the District 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. The Contractor represents and warrants that it will comply with the District's data security and privacy policy and other applicable policies.

6. Right of Review and Audit.

Upon request by the District, the Contractor will provide the District with copies of its policies and related procedures that pertain to the protection of PII and District Data. The policies and procedures may be made available in a manner that does not violate Contractor's own information security policies, confidentiality obligations, and applicable laws. In addition, Contractor may be required by the District to undergo an audit of Contractor's privacy and security safeguards, measures and controls as they pertain to alignment with the requirements of applicable New York, federal and local laws, rules and regulations, the District policies applicable to the Contractor, and alignment with the NIST Cybersecurity Framework performed by an independent third party at the Contractor's expense, and provide the written audit report to the District. The Contractor may provide the District with a recent industry standard audit report performed by an independent third party on the Contractor's privacy and security practices as an alternative to undergoing an audit. The determination of whether the previously prepared audit report is "recent" will be determined by the District in its sole judgment.

7. Access to/Disclosure of District Data

(a) The Contractor agrees that it will limit the Contractor's internal access to and only Disclose PII to the Contractor's officers, employees and Subcontractors who need to access the PII in order to provide the Services and that the disclosure of PII will be limited to the extent necessary to provide the Services pursuant to the Service Agreement. The Contractor must take all actions necessary to ensure that all its officers, employees and Subcontractors comply with the terms of this DPA.

(b) The Contractor must ensure that each Subcontractor performing functions pursuant to the Service Agreement where the Subcontractor will receive or have access to District Data must be 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) The Contractor must examine the data security and privacy measures of its Subcontractors prior to utilizing the Subcontractor to ensure compliance with this DPA. If at any point a Subcontractor fails to materially comply with the requirements of this DPA, the Contractor must: notify the District and prevent the Subcontractor's continued access to District Data; and, as applicable, retrieve all District Data received or stored by Subcontractor and/or ensure that District Data has been securely deleted and destroyed in accordance with this DPA. In the event there is an incident in which the Subcontractor compromises PII, the Contractor must follow the Data Breach reporting requirements set forth herein.

(d) The Contractor will take full responsibility for the acts and omissions of its officers, employees and Subcontractors.

(e) The Contractor must not Disclose District Data to any other party (a party other than the Contractor's officers or employees or Subcontractors who does not need access to the District Data to provide the Services pursuant to the Service Agreement) without the prior written consent of the District (if necessary, the District will obtain the required consent(s) from third parties) unless the disclosure is required by statute, court order or subpoena, and the Contractor makes a reasonable effort to notify the District of the court order or subpoena in advance of compliance but in any case, provides notice to the District no later than the time the District Data is disclosed, unless such disclosure to the District is expressly prohibited by the statute, court order or subpoena.

(f) Except as prohibited by law, the Contractor will: (i) immediately notify the District of any subpoenas, warrants, or other legal orders, demands or requests received by the Contractor seeking District Data; (ii) consult with the District regarding the Contractor's response; (iii) cooperate with the District's reasonable requests in connection with efforts by the District to intervene and quash or modify the legal order, demand or request; and (iv) upon the District's request, provide the District with a copy of the Contractor's response.

(g) Upon the District's request, the Contractor agrees that it will promptly make any District Data held by the Contractor available to the District.

8. Training.

The Contactor must ensure that all its officers, employees and Subcontractors who have access to PII have received or will receive training on the federal and State laws governing confidentiality of the data prior to receiving access.

9. Term and Termination.

This DPA will be effective as of the date the Service Agreement is effective and will terminate on the termination of the Service Agreement. However, the obligations of the parties pursuant to this DPA will survive the expiration of the Service Agreement and will continue until the Contractor and Subcontractors no longer retain PII and no longer retain access to PII.

10. Data Return and Destruction of Data.

(a) Protecting PII from unauthorized access and disclosure is of the utmost importance to the District, and the 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 District, unless such retention is expressly authorized for a prescribed period by the Service Agreement or other written agreement between the Parties, expressly requested by the District for purposes of facilitating the transfer of PII to the District or expressly required by law. As applicable, upon expiration or termination of

the Service Agreement, the Contractor will transfer PII, in a format agreed to by the Parties to the District.

(b) If applicable, once the transfer of PII has been accomplished in accordance with the District's written election to do so, the Contractor agrees to return or destroy all PII when the purpose that necessitated its receipt by the Contractor has been completed. Thereafter, with regard to all PII (including without limitation, all hard copies, archived copies, electronic versions, or electronic imaging of hard copies) as well as any and all PII maintained on behalf of the Contractor in a secure data center and/or in cloud-based facilities that remain in the possession of the Contractor or its Subcontractors, the Contractor will 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) The Contractor will provide the District with a written certification of the secure deletion and/or destruction of PII held by the Contractor or Subcontractors.

(d) To the extent that the 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), the Contractor agrees not to attempt to re-identify de-identified data and not to transfer de-identified data to any party.

11. Commercial or Marketing Use Prohibition.

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

12. Encryption.

The Contractor will 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 in transit in accordance with applicable New York laws and regulations.

13. Storage.

Contractor must store all District Data within the United States of America.

14. Breach.

a. The Contractor must promptly notify the District of any Breach of PII in the most expedient way possible and without unreasonable delay and in no event more than seven calendar days after discovery of the Breach. Notifications required pursuant to this section must be in writing and by email (if email address is provided) and personal delivery or nationally recognized overnight carrier. Notifications 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 District. Violations of the requirement to notify the District are subject to civil penalty(ies) pursuant to Education Law § 2-d. The Breach of certain PII protected by Education Law §2-d may subject the Contractor to additional penalties.

b. Notifications required to be made to the District pursuant to this paragraph must be sent to the following people at the following addresses:

Dr. Jordan Cox
Superintendent of Schools
Commack Union Free School District
PO Box 150
Commack, NY 11725
Email: jcox@commack.k12.ny.us

Mrs. Alise Pulliam
Executive Director for Instructional Technology
Commack Union Free School District
PO Box 150
Commack, NY 11725
Email: apulliam@commack.k12.ny.us

15. Cooperation with Investigations.

Contractor agrees that it will cooperate with the District 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' officers, employees or Subcontractors, as related to such investigations, will be the sole responsibility of the Contractor if the Breach is attributable to Contractor or its Subcontractors.

16. Notification to Individuals.

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

ARTICLE III: PARENT AND ELIGIBLE STUDENT PROVISIONS

1. Parent and Eligible Student Access.

Education Law § 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 District. To the extent Student Data is held by the Contractor pursuant to the Service Agreement, the Contractor must respond within 20 calendar days to the District's requests for access to Student Data so the District can facilitate 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 the Contractor pursuant to the Service Agreement, the Contractor must promptly notify the District and refer the Parent or Eligible Student to the District.

2. Bill of Rights for Data Privacy and Security.

As required by Education Law § 2-d, the Parents Bill of Rights for Data Privacy and Security and the supplemental information for the Service Agreement are annexed hereto as Exhibit A and Exhibit B, respectively, and incorporated into this DPA. The Contractor must complete and sign Exhibits A and B. Pursuant to Education Law § 2-d, the District 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 will govern and prevail, will survive the termination of the Service Agreement in the manner set forth herein, and supersedes 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 will 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 will be and constitute an original signature, as if all parties had executed a single original document.

Commack Union Free School District	Goosechase Adventures Inc.
By: (Signature)	By: (Signature) Stylianoudis
Alise Pulliam	(Printed Name) Alexander Stylianoudis
Executive Director for Instructional Technology	(Title) Head of Legal & Finance
Date: 4/8/2024	Date: 01/02/2024

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

COMMACK UNION FREE SCHOOL DISTRICT

PARENTS' BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY –

Summary of Rights and Information for Parents and Students

The legislature and governor passed a group of bills that adjusted the Regents Education Reform Agenda. These bills are known collectively as the "Common Core Implementation Reform Act." One of the key components of this act (Chapter 56, Part AA, Subpart L, of the laws of 2014) directs the Commissioner of Education to appoint a Chief Privacy Officer (CPO). A major function of this new position is to work with school districts and parents to develop elements for a parents' bill of rights to help ensure that student data is private and secure. The State Education Department (SED) and the CPO must also recommend regulations to establish standards for data security and privacy policies that will be implemented statewide.

SED has issued a preliminary Parents' Bill of Rights for Data Privacy and Security. The Commack Union Free School District is issuing this summary of parents' rights under the new law. While some additional elements will be developed in conjunction with the CPO, districts, parents and the Board of Regents, this summary sets forth the key rights and information that parents should be aware of in regards to ensuring the privacy and security of their student's educational data.

The Commack Union Free School District is committed to ensuring student privacy and recognizes that parents, legal guardians, and persons with a parental relationship to a student are entitled to certain rights with regard to their child's personally identifiable information, as defined by Education Law §2-d. To this end, the District is providing the following Parent's Bill of Rights for Data Privacy and Security:

1. A student's personally identifiable information cannot be sold or released for any commercial purposes;

2. Parents have the right to inspect and review the complete contents of their child's education record;

3. State and federal laws protect the confidentiality of personally identifiable information, and safeguards associated with industry standards and best practices, including but not limited to, encryption, firewalls, and password protection, must be in place when data is stored or transferred;

4. A complete list of all student data elements collected by the State is available for public review at http://www.p12.nysed.gov/irs/sirs/documentation/NYSEDstudentData.xlsx or by

writing to the Office of Information & Reporting Services, New York State Education Department, Room 863, 89 Washington Avenue, New York 12234; and

5. Parents and guardians have the right to have complaints about possible breaches of student data addressed. Complaints should be addressed to Alise Pulliam, Executive Director for Instructional Technology, PO Box 150, Commack, New York 11725, Phone: (631) 912-2027, Email: alisepulliam@commack.k12.ny.us or Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, New York 12234.

If the Commack Union Free School District enters into a third-party contract in which the service provider receives student data or teacher or principal data in order to provide a needed service for the District, supplemental information shall be developed and provided to parents that states:

6. The exclusive purposes for which the student data or teacher or principal date will be used;

7. How the third-party contractor will ensure that the subcontractors, persons or entities that the third-party contractor will share the student data or teacher or principal data with, if any, will abide by data protection and security requirements;

8. When the agreement expires and what happens to the student data or teacher or principal data upon expiration of the agreement;

9. If and how a parent, student, eligible student, teacher or principal may challenge the accuracy of the student data or teacher or principal data that is collected; and

10. Where the student data or teacher or principal data will be stored and the security protections taken to ensure such data will be protected, including whether such data will be encrypted.

The CPO as appointed by the Commissioner must secure input from parents and other education and expert stakeholders to develop additional elements for the Parents' Bill of Rights for Data Privacy and Security. The Commissioner of Education will also be promulgating regulations with a comment period for parents and other members of the public to submit comments and suggestions to the CPO.

In the meantime, you can access additional information and a question and answer document issued by SED as a preliminary Parents' Bill of Rights for Data Privacy and Security.

If you have any further questions or concerns at this time, please contact Dr. Jordan Cox, Superintendent, Commack UFSD, PO Box 150, Commack, New York 11725 or Mrs. Alise Pulliam at apulliam@commack.k12.ny.us

By: (Signature) Stylianoudis
(Printed Name) Alexandre Stylianoudis
(Title) Head of Legal & Finance
Date: 02/01/2024

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 8 NYCRR § 121.3, the District is required to post information to its website about its contracts with third-party contractors ("Service Agreements") that will receive Personally Identifiable Information ("PII") from Student Data or Teacher or Principal APPR Data.

	Goosechase Adventures Inc.
Term of Service Agreement	Agreement Start Date: December 1st, 2023 Agreement End Date: June 30th, 2026
Description of the purpose(s) for which Contractor will receive/access/use PII	PII received by the Contractor will be received, accessed and used only to perform the Contractor's Services pursuant to the Service Agreement with the District. List Purposes: Our platform ingests a range of mandatory and optional data. For mandatory data, this is typically limited to IP addresses and the email address of the game organizer, as well as any additional information required for contact or billing purposes. For optional data, this is highly dependent on how games are set up and participants join the game.
Type of PII that Contractor will receive/access	Check all that apply: ☒ Student PII — If and only if students are instructed to create an account, which they should do as we have the "play as guest" option ☐ Teacher or Principal APPR Data
Subcontractor Written Agreement Requirement	The Contractor will only share PII with entities or persons authorized by the Service Agreement. The Contractor will not utilize Subcontractors without written contracts that require 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 Service Agreement. Check applicable option. ☒ Contractor will not utilize Subcontractors.

	☐ Contractor will utilize Subcontractors.
Data Transition and Secure Destruction	Upon expiration or termination of the Service Agreement, the Contractor will, as directed by the District in writing: • Securely transfer data to District, or a successor contractor at the District's option and written discretion, in a format agreed to by the parties. • Securely delete and destroy data by taking actions that render data written on physical (e.g., hard copy) or electronic media unrecoverable by both ordinary and extraordinary means.
Challenges to Data Accuracy	Parents, students, teachers or principals who seek to challenge the accuracy of PII will do so by contacting the District. If a correction to data is deemed necessary, the District will notify the Contractor. The Contractor agrees to facilitate such corrections within 21 calendar days of receiving the District's written request.
Secure Storage and Data Security	The Contractor will store and process District Data in compliance with § 2-d(5) and applicable regulations of the Commissioner of Education, as the same may be amended from time to time, and in accordance with commercial best practices, including appropriate administrative, physical and technical safeguards, to secure district Data from unauthorized access, disclosure, alteration and use. The Consultant will use legally-required, industry standard and up-to-date security tools and technologies such as anti-virus protections and intrusion detection methods in providing services pursuant to the Service Agreement. The Contractor will conduct periodic risk assessments and remediate any identified security vulnerabilities in a timely manner. Please describe where PII will be stored and the security protections taken to ensure PII will be protected and data security and privacy risks mitigated in a manner that does not compromise the security of the data: (a) Storage of Electronic Data (check all that apply): ☒ Using a cloud or infrastructure owned and hosted by a third party. ☐ Using Contractor owned and hosted solution

	☐ Other: (b) Storage of Non-Electronic Data: all data is electronic (c) Personnel/Workforce Security Measures: Access of PII is very much limited on a need basis, access are logged and audited (d) Account Management and Access Control: similar to above, all passwords are stored on 1password, where logs and adutis are periodically made (e) Physical Security Measures: we're full remote not applicable (f) Other Security Measures: please see security documentation
Encryption	Data will be encrypted while in motion

By: (Signature)	Stylianoudis
(Printed Name)	Alexandre Stylianoudis
(Title)	Head of Legal and Finance
Date:	02/01/2024

EXHIBIT C - CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

The Commack Union Free School District 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. 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. The terms of the plan cannot conflict with any other terms of or Exhibits to the Data Privacy Agreement to which this Exhibit C is attached. **While this plan is not required to be posted to the District's website, contractors should nevertheless ensure that they do not include information that could compromise the security of their data and data systems. DO NOT LIMIT RESPONSES TO THE SPACES PROVIDED.**

1	Outline how you will implement applicable data security and privacy contract requirements over the life of the Contract	please see security documentation
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	please see security documentation
3	Specify how your officers, employees and Subcontractors who have access to PII pursuant to the Service Agreement will receive training on the federal and State laws that govern the confidentiality of PII.	please see security documentation
4	Outline the processes that ensure that your officers, employees and Subcontractors are bound by written agreement to the requirements of the Service Agreement, at a minimum.	please see security documentation
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 District.	please see security documentation

6	Describe how data will be transitioned to the District when no longer needed by you to meet your contractual obligations, if applicable.	please see security documentation
7	Describe your secure destruction practices and how certification will be provided to the District.	please see security documentation
8	Outline how your data security and privacy program/practices align with the District's applicable policies.	please see security documentation
9	Outline how your data security and privacy program/practices materially align with the NIST CSF v1.1 using the Framework chart below.	***YOU MAY 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.	Yes
	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	Yes - further documentation available
	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.	Yes - further documentation available
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	Yes
	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	Yes

PROJECT (PR)	**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 processes to identify, assess and manage supply chain risks.	Yes - further documentation available Yes - further documentation available
	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.	servers are hosted with AWS
	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.	Yes
	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.	Yes - further documentation available
	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.	Yes please see documentation attached
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	Yes please see documentation attached
	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.	Yes additonal documentation available
	Anomalies and Events (DE.AE):	Yes please see documentation attached

DETECT (DE)	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.	Yes please see documentation attached
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	Yes please see documentation attached
RESPOND (RS)	**Response Planning (RS.RP):** Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.	Yes please see documentation attached
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	Yes additonal documentation available
	Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.	Yes please see documentation attached
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	Yes please see documentation attached
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	Yes please see documentation attached
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.	Yes please see documentation attached
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	Yes please see documentation attached
	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).	Yes please see documentation attached

goosechase
Security Features

1. Product Information

- What is Goosechase?
- Types of Accounts
- How is data being processed?

2. Encryption

- General data encryption
- Backup encryption
- Crypto and key management scheme used
- Admin access

3. Server and Application Interface Security

- Data storage
- Protection of the production environment
- Application and supporting infrastructure design

4. Third Party

- Third party processors
- Transfer of data
- GDPR policy

5. Data Retention & Deletion

- Data retention
- Date deletion
- Backups
- Termination of the service agreement

6. Audit and Compliance

- Security vulnerabilities
- Privacy breaches
- Security Development

7. Change Control

Logging activities & log safeguards
Change control process

8. Human Resources

Accountability for cyber security and security testing program
Security team
Team
Team training
Termination

9. Infrastructure and Virtualization Security

Segregation of environments

10. Identity and Access Management

Endpoint protection controls
Restriction, log and monitoring access to our systems
Ensuring that access to data is granted on as-needed basis
Do you use multi-factor authentication for all privileged access?
Preventing unauthorized access to systems, applications, users' data or source code
Process for granting and documenting approval for access of tenant data

11. Incident Management

Incident management process
Monitoring infrastructure for identification of events related to specific users
Enforcing and attesting to tenant data separation when producing data in response to legal subpoenas
Contact in the unlikely event it would be needed

12. Integration

Ways to safe-list the application
Methods to integrate with other SaaS or on-premise systems
RESTful APIs via an API Gateway
Method of sending email notifications (to registrants & staff) from this system

Product Information

What is Goosechase?

At Goosechase, experience is everything. Originally inspired by scavenger hunts, Goosechase is an online platform that enables organizations and schools to engage, activate, and educate their communities through delightful interactive experiences.

Created online but played in the real world, Goosechase brings communities to life with engaging, interactive challenges designed to support organizations. The intuitive platform makes it easy to make a repeatable, fun, and positive impact on any community.

Since hatching in Canada in 2011, Goosechase has powered hundreds of thousands of global team building, training, fundraising, educational, tourist, and recreational experiences.

Types of Accounts

Play as Guest;
The Play as a Guest option allows users to play without the need to create a Goosechase account. When participants select this option, they will be taken directly to the Join an Experience window and prompted to find their Experience by name or Join code in order to find and join an Experience as usual.

By playing as a Guest, their activity is only saved to their mobile device, and will not be saved to an online account. This activity will be deleted if they uninstall the Goosechase app from their device or reset the app from the settings menu.

For the avoidance of doubt, Goosechase will not collect any personally identifiable information through this option

Create an Account
Playing with an account allows a participant to tie all their activity to that account. Once an account is created, a participant can even sign in from another device to access all their data. To sign up, a user will only need to create a username, chose their password, and add their email address. No other personally identifiable information will be requested to either create or maintain an account.

How is data being processed (i.e. who has access to customer data?)

Our platform ingests a range of mandatory and optional data.

For mandatory data, this is typically limited to IP addresses and the email address of the creator, as well as any additional information required for contact or billing purposes.

For optional data, this is highly dependent on how Experiences are set up and participants join. If Participants Play as Guest, data collected will be usage-based data whereas if they register for an account, it will be usage data and their email address.

Within the Experience, the type of data collected will be entirely contingent on the missions that are designed by the creator..

Encryption

How is data encrypted?

All customer data is encrypted during transit using TLS and SSL, with passwords salted and hashed. Given the lack of sensitive data that we collect, we currently do not encrypt data at rest. However, encryption at rest will be implemented in the second half of 2022 ahead of exciting new features.

How are admin systems accessed?

Accessing admin systems for our infrastructure requires 2FA, and accessing individual servers requires SSH key, password, and 2FA.

Backup encryption

Backups are encrypted in transit and at rest.

Crypto and key management scheme used

Passwords are salted and hashed.

Server and Application Interface Security

Data location, access and storage

Our platform is hosted on a combination of AWS and Linode infrastructure. Our staging environment is fully isolated and physically separated from our production environment and contains no customer data. As both servers are fully separate, hosted by two vastly different companies, the breach of one environment would not contaminate the other.

Ensuring that only tested and non-malicious code is released to production

Before any code is deployed, it needs to undergo a thorough code review by at least one other member of our team, along with complimentary automated testing. We use Automated unit testing, manual testing prior to release, segmented rollouts, exception and error tracking before any code is deployed

Application and supporting infrastructure design

Our backend infrastructure runs on virtualized Ubuntu servers powered by Linode. We use industry-standard practices for access control, in-flight encryption, and firewalling to ensure the security of our infrastructure and data. We also use full-disk backups to enable quick and effective recoveries in the case of data loss.

Third Party

List of other vendors or third party that may have access to tenant data or any subset of the data

Our full subprocessor list, along with the purpose of each, is available at: https://www.goosechase.com/sub-processors

Do we share data?

In general, we only ever share data with a third party for a specific purpose, such as improving our product through anonymized usage analytics. For anything related to advertising/marketing, we only share information upon explicit user opt-in on our website and that is only for customer acquisition - no user data is ever monetized.

GDPR policy

Please find our GDPR Policy here: https://www.goosechase.com/privacy

Data Retention & Deletion

Defined data retention periods

Our accounts are designed to have a full history for ease of use. For the complete removal of information, the account would need to be deleted.

Procedure upon termination of the service agreement

Users can request to have their data deleted at any moment within the app, by sending an email to hi@goosechase.com or submitting a form through https://privacy.saymine.io/Goosechase_Adventures_Inc. Upon receiving a data deletion request, from the app, form or email, the user's third-party data will also be deleted (if applicable)

Before permanently deleting their data, users would be able to export their data, including any submissions (videos or photos) as well as the data gathered to date.

Deletion methodology

When we receive a request asking for total data deletion, we just wipe it out of our database, and from our backups. Our systems would also delete their data from other software in which their data may be held, such as Mixpanel or Intercom.

Backup deletion frequency

Backups are kept indefinitely unless a user specifically requests permanent data deletion. Upon receiving any data deletion requests, the process described above would also include data deletion from our backups.

Audit and Compliance

Assessing the application for security vulnerabilities prior to production deployment

As part of our development processes, we regularly audit all third-party libraries for updated versions and security patches. Our build process also automatically audits our libraries for known vulnerabilities. We also use automated vulnerability scanning and other manual testing.

Monitoring privacy breaches

We have intrusion sensors and 24x7 real-time automated monitoring systems for log-ins. We have a rotation system that ensures that someone can be paged and act upon any intrusion in the briefest delays. We also have log safeguards so that our CTO can go back historically in system and application logs to forensically identify the causes of a breach in both production and staging environments. Our incident response procedure may be shared upon contacting alex@goosechase.com

Security development

The application development follows OWASP top ten, and we follow industry best practices across the board.

Change Control

Logging activities & log safeguards

We have an automated monitoring system for log-ins, along with log safeguards so that one can go back historically in system and application logs to forensically identify the causes of breaches in both production and staging environments.

Frequency of back up of critical IT systems and sensitive data

Our backup is run automatically every 24hrs.

Change control process

We use a Git repository for tracking changes in any set of files, and we have the ability to do rollbacks on any changes performed.

Human Resources

Accountability for cyber security and security testing program

Logan Fuller, our CTO & CISO.

Security team

Logan is both our Chief Information Security Officer, as well as our Chief Technology Officer. He would report to the board, including Alyshahn, our CRO, and Andrew, our CEO. The security team currently comprises of Logan, Alexander (head of legal), and another senior engineer.

Team

We have a small team of developers. Duties are separated to reduce the opportunity for unauthorized modification, unintentional modification or misuse of the organization's IT assets.

Team training

Every team member is rigorously tested on these matters ahead of hiring and extensively trained throughout their onboarding period to cover all bases. Periodic training and continuous learning on security issues as well as other cyber security matters are also performed when and if needed.

Termination

Upon termination, employees are revoked access from all platforms as they are being communicated the information. Their access to their email, workspace, password manager, project management software, slack, and any other systems are simultaneously revoked. Upon termination, we always pay their termination notice forward so that they do not need to work for us in the interim.

Infrastructure and Virtualization Security

Segregation between production and non production environments

Both Production and non-production environments are entirely firewalled, one cannot access the other, making them entirely segregated.

Separation

System and network environments are both protected and separate by a firewall.

Identity and Access Management

Endpoint protection controls

We use firewall authentication and validation systems for every system connected to our infrastructure.

Restriction, log and monitoring access to our systems

All authentication attempts to our platform, successful or otherwise, are logged. We also fully log all requests to our service, though we do not specifically audit or log access to customer data or changes to security configurations.

Ensuring that access to data is granted on as needed basis

Team members do not have access to any user's unencrypted data unless explicitly required to perform a function that is a direct benefit to the user such as upgrading an account, an Experience or providing contextual support.

Do you use multi factor authentication for all privileged access?

Single sign-on protocols and multi-factor authentication are not currently supported.

Preventing unauthorized access to systems, applications, users' data or source code

One's data can be ingested via our website or mobile applications. In both interfaces, all requests require authorized accounts with the appropriate permissions for all data types and are carried out over TLS connections. We also rate-limit login attempts based on IP.

Process for granting and documenting approval for access of tenant data

Accounts are initially authorized via username/email and password combinations, with appropriate per-user API keys being returned for all future requests. All passwords are fully salted and hashed before being stored in our database and are never transmitted, stored, or logged in plaintext.

Incident Management

Incident management process

Our lengthy incident management documentation can be accessed by contacting alex@goosechase.com

Monitoring infrastructure for identification of events related to a specific users

Our monitoring infrastructure allows for the identification of events related to a specific user.

Enforcing and attesting to tenant data separation when producing data in response to legal subpoenas

Our head of legal operations would handle all subpoenas and/or court orders. Any process would follow and be aligned with any local jurisdictions, as well as our own in Ontario.

Contact in the unlikely event it would be needed

It's very likely that should any issues arise, our team will be aware of them and contact you proactively. However, if a security incident does arise and you need to contact us, you can contact our CRO directly at alyshahn@goosechase.com or 647 984 7806.

In the matter of a security incident, you can expect a response immediately. You will be made aware if there is a different point of contact at any point during the course of our partnership.

Integration

Ways to safe-list the application

IPs are 104.200.22.31 and 2600:3c00:1::68c8:161f, though ideally just safe-listing *.goosechase.com should do as we have a dynamic address.

Methods to integrate with other SaaS or on-premise systems

Direct API access.

RESTful APIs via an API Gateway

We don't use a Gateway but we can consume Restful API.

Method of sending email notifications (to registrants & staff) from this system

Email notifications are sent via Grid as well as Intercom.

goosechase

EXECUTIVE SUMMARY

To maintain the trust of our employees, customers, and partners and meet regulatory requirements, it is essential that we do everything we can to protect confidential information and systems in the face of a cyberattack. The better prepared we are to respond to a potential cyberattack, the faster we can eradicate any threat and reduce the impact on our business.

This document describes the plan for responding to information security incidents at GooseChase Adventures Inc ("**GooseChase**"). This document will explain how to detect and react to cybersecurity incidents and data breaches, determine their scope and risk, respond appropriately and quickly, and communicate the results and risks to all stakeholders.

Effective incident response involves every part of our organization, including IT teams, legal, technical support, human resources, corporate communications, and business operations. It is important that you read and understand your role as well as the ways you will coordinate with others.

This plan will be updated at least annually to reflect organizational changes, new technologies and new compliance requirements that inform our cybersecurity strategy. We will conduct regular testing of this plan to ensure everyone is fully trained to participate in effective incident response.

ROLES, RESPONSIBILITIES & CONTACT INFORMATION
This Security Incident Response Plan must be followed by all personnel, including all employees, temporary staff, consultants, contractors, suppliers and third parties operating on behalf of GooseChase All personnel are referred to as 'staff' within this plan.

Below are details about the roles and responsibilities of each member of GooseChase to prevent and respond to a workplace incident. It is not an exhaustive list of duties but designed to give each employee a general understanding of their role and the roles of other employees in incident response and prevention.

Incident Response Team Responsibilities

The Incident Response Lead is responsible for:

- Making sure that the Security Incident Response Plan and associated response and escalation procedures are defined and documented. This is to ensure that the handling of security incidents is timely and effective.
- Making sure that the Security Incident Response Plan is current, reviewed and tested at least once each year.
- Making sure that staff with Security Incident Response Plan responsibilities are properly trained at least once each year.
- Leading the investigation of a suspected breach or reported security incident and initiating the Security Incident Response Plan when needed.
- Reporting to and liaising with external parties, including pertinent business partners, legal representation, law enforcement, etc., as is required.
- Authorizing on-site investigations by appropriate law enforcement or third-party security/forensic personnel, as required during any security incident investigation. This includes authorizing access to/removal of evidence from site.

Security Incident Response Team (SIRT) members are responsible for:

- Making sure that all staff understand how to identify and report a suspected or actual security incident.
- Advising the Incident Response Lead of an incident when they receive a security incident report from staff.
- Investigating and documenting each reported incident.
- Taking action to limit the exposure of sensitive data and to reduce the risks that may be associated with any incident.
- Gathering, reviewing, and analysing logs and related information from various central and local safeguards, security measures and controls.
- Documenting and maintaining accurate and detailed records of the incident and all activities that were undertaken in response to an incident.
- Assisting law enforcement during the investigation processes. This includes any forensic investigations and prosecutions.

- Initiating follow-up actions to reduce likelihood of recurrence, as appropriate.
- Determining if policies, processes, technologies, security measures or controls need to be updated to avoid a similar incident in the future. They also need to consider whether additional safeguards are required in the environment where the incident occurred.

All staff members are responsible for:

- Making sure they understand how to identify and report a suspected or actual security incident.
- Reporting a suspected or actual security incident to the Incident Response Lead (preferable) or to another member of the Security Incident Response Team (SIRT).
- Reporting any security related issues or concerns to line management, or to a member of the SIRT.
- Complying with the security policies and procedures of GooseChase

Roles, Responsibilities and Contact Information

ROLE	RESPONSIBILITY	CONTACT DETAILS
INFORMATION SECURITY		
CSO / CISO	Strategic lead. Develops technical, operational, and financial risk ranking criteria used to prioritize incident response plan. Authorizes when and how incident details are reported. Main point of contact for executive team and Board of Directors.	Name: Logan Fuller Email: Logan@goosechase.com
Incident Response Team Lead and Team Members	Central team that authorizes and coordinates incident response across multiple teams and functions through all stages of a cyber incident.	Name: Logan Fuller Email: Logan@goosechase.com
	Maintains incident response plan, documentation, and catalog of incidents.	Name: Alexandre Stylianoudis Email: alex@goosechase.com
	Responsible for identifying, confirming, and evaluating extent of incidents.	Name: Alyshahn Kara Virani Email: Alyshahn@goosechase.com

	Conducts random security checks to ensure readiness to respond to a cyberattack.	
Identity and Access Team Lead and Team Members	Responsible for privilege management, enterprise password protection and role-based access control. Discovers, audits, and reports on all privilege usage. Conducts random checks to audit privileged accounts, validate whether they are required, and re-authenticate those that are. Monitors privileged account uses and proactively checks for indicators of compromise, such as excessive logins, or other unusual behavior. Informs incident response team of potential attacks that compromise privileged accounts, validates and reports on the extent of attacks. Takes action to prevent the spread of a breach by updating privileges.	Name: Logan Fuller Email: Logan@goosechase.com
IT Operations and Support (internal)	Manages access to systems and applications for internal staff and partners. Centrally manages patches, hardware and software updates, and other system upgrades to prevent and contain a cyberattack.	Name: Logan Fuller Email: Logan@goosechase.com
COMPLIANCE		
Legal Counsel	Confirms requirements for informing employees, customers, and the public about cyber breaches. Responsible for checking in with local law enforcement.	Name: Alexandre Stylianoudis Email: alex@goosechase.com

	Ensures IT team has legal authority for privilege account monitoring.	
Audit & Compliance	Communicates with regulatory bodies, following mandated reporting requirements.	Name: Alexandre Stylianoudis Email: alex@goosechase.com

COMMUNICATIONS

Marketing & Public Relations Lead	Communicates externally with customers, partners, and the media. Coordinates all communications and request for interviews with internal subject matter experts and security team. Maintains draft crisis communications plans and statements which can be customized and distributed quickly in case of a breach.	Name: Katie Canton Email: katie@goosechase.com

Testing and Updates

Annual testing of the Incident Response Plan using walkthroughs and practical simulations of potential incident scenarios is necessary to ensure the SIRT are aware of their obligations, unless real incidents occur which test the full functionality of the process.

1. The Incident Response Plan will be tested at least once annually.
2. The Incident Response Plan Testing will test [your business]'s response to potential incident scenarios to identify process gaps and improvement areas.
3. The SIRT will record observations made during the testing, such as steps that were poorly executed or misunderstood by participants and those aspects that need improvement.
4. The Incident Response Lead will ensure the Security Incident Response Plan is updated and distributed to SIRT members.

INCIDENT RESPONSE PROCESS OVERVIEW

Below is the structured 6-step process followed in this document as defined by the SANS Institute in their Incident Handler's Handbook. The six steps outlined are:

1. **Preparation**—review and codify an organizational security policy, perform a risk assessment, identify sensitive assets, define which are critical security incidents the team should focus on, and build a Computer Security Incident Response Team (CSIRT).

2. **Identification**—monitor IT systems and detect deviations from normal operations and see if they represent actual security incidents. When an incident is discovered, collect additional evidence, establish its type and severity, and document everything.

3. **Containment**—perform short-term containment, for example by isolating the network segment that is under attack. Then focus on long-term containment, which involves temporary fixes to allow systems to be used in production, while rebuilding clean systems.

4. **Eradication**—remove malware from all affected systems, identify the root cause of the attack, and take action to prevent similar attacks in the future.

5. **Recovery**—bring affected production systems back online carefully, to prevent additional attacks. Test, verify and monitor affected systems to ensure they are back to normal activity.
6. **Lessons learned**—no later than two weeks from the end of the incident, perform a retrospective of the incident. Prepare complete documentation of the incident, investigate the incident further, understand what was done to contain it and whether anything in the incident response process could be improved.

Escalation plan

Emergency Incident

- Definition: "Emergency Incident": an incident which fully or partially prevents usability of the platform or severely impairs the operations.
- Response time: no later than the day of receiving the incident report within regular EST business hours.
- Resolution time: GooseChase to commences incident resolution within one business day and assigns its employees to this task until the incident has been resolved or an acceptable "workaround" has been found for the customer.

High Priority Incident;

- Definition; High Priority Incident: an incident which neither prevents usability of the platform nor severely impairs the customer's productive operations, but limits usability of the platform and has a significant impact on the productive operations.
- The impact on the productive operations can be reduced to a tolerable level through appropriate workaround measures.
- Response time: no later than the day after receiving the incident report within regular EST business hours
- Resolution time: GooseChase commences incident resolution within two business days and assigns its employees to this task until the incident has been resolved or an acceptable "workaround" has been found for the customer.

Normal Priority Incident

- Definition; "Normal Priority Incident": an incident which impairs the use of contractual services and has only a limited impact on the productive operations (business processes).
- "Response time": within three business days after receiving the incident report "Resolution time": GooseChase sends an initial response to the incident report requesting further information or clarification within five business days after receiving the incident report. GooseChase will also take into account a "workaround" as well as platform improvements which resolve the incident in a subsequent update.

Minor Priority Incident:

- Definition; an incident which impairs the use of contractual services and has only a minimal, limited impact on the customer's productive operations (business processes).
- These incidents do not significantly impair usability of the platform. They will be resolved during regular development as part of the next release.

Incident Response Checklist

To demonstrate and improve the effectiveness of GooseChase incident response team and security tools, GooseChase requires a record of all actions taken during each phase of an incident. Supporting documentation is required, including all forensic evidence collected such as activity logs, memory dumps, audits, network traffic, and disk images.

TASK OF INCIDENT	ACTION	TEAM MEMBER/ SYSTEM	DAY/TIME ACTION TAKEN
Incident Discovery and Confirmation	Describe how the team first learned of the attack (security researcher, partner, employee, customer, auditor, internal security alert, etc.). Analyze audit logs and security applications to identify unusual or suspicious account behavior or activities that indicate a likely attack and confirm attack has occurred. Describe potential attacker, including known or expected capabilities, behaviors, and motivations. Identify access point and source of attack (endpoint, application, malware downloaded, etc.) and responsible party. Prepare an incident timeline to keep an ongoing record of when the attack occurred and subsequent milestones in analysis and response. Check applications for signatures, IP address ranges, files hashes, processes, executables names, URLs, and domain names of known malicious websites. Evaluate extent of damage upon discovery and risk to systems and privileged accounts. Audit which privileged accounts have been used recently, whether any passwords have been changed, and what applications have been executed. (See Appendix A for more information on Threat Classification). Review your information assets list to identify which assets have been potentially compromised. Note integrity of assets and evidence gathered. (See Appendix A for more information on Threat Classification). Diagram the path of the incident/attack to provide an "at-a-glance" view from the initial breach to escalation and movement tracked across the network.		

	Collect meeting notes in a central repository to use in preparing communications with stakeholders.
	Inform employees regarding discovery.
	Analyze incident Indicators of Compromise (IOCs) with threat intelligence tools.
	Potentially share information externally about breach discovery. You may choose to hold communications during this phase until you have contained the breach to increase your chances of catching the attacker. If so, make sure this aligns with your compliance requirements.
Containment and Continuity	Enable temporary privileged accounts to be used by the technical and security team to quickly access and monitor systems.
	Protect evidence. Back up any compromised systems as soon as possible, prior to performing any actions that could affect data integrity on the original media.
	Force multi-factor authentication or peer review to ensure privileges are being used appropriately.
	Change passwords for all users, service, application, and network accounts.
	Increase the sensitivity of application security controls (allowing, denying, and restricting) to prevent malicious malware from being distributed by the attacker.
	Remove systems from production or take systems offline if needed.
	Inform employees regarding breach containment.
	Analyze, record, and confirm any instances of potential data exfiltration occurrences across the network.
	Potentially share information externally regarding breach containment (website updates, emails, social media posts, tech support bulletins, etc.).
Eradication	Close firewall ports and network connections.
	Test devices and applications to be sure any malicious code is removed.
	Compare data before and after the incident to ensure systems are reset properly.
	Inform employees regarding eradication.
	Potentially share information externally regarding eradication (website updates, emails, social media posts, tech support bulletins, etc.).

Recovery	Download and apply security patches.
	Close network access and reset passwords.
	Conduct vulnerability analysis.
	Return any systems that were taken offline to production.
	Inform employees regarding recovery.
	Share information externally regarding recovery (website updates, emails, social media posts, tech support bulletins, etc.).
Lessons Learned	Review forensic evidence collected.
	Assess incident cost.
	Write an Executive Summary of the incident.
	Report to executive team and auditors if necessary.
	Implement additional training for everyone involved in incident response and all employees.
	Update incident response plan.
	Inform employees regarding lessons learned, additional training, etc.
	Potentially share information externally (website updates, emails, social media posts, tech support bulletins, etc.).

Responsibilities At-a-Glance

Activity	**Role**				
	CSIRT Incident Lead	**IT Contact**	**Legal Representative**	**Communications Officer**	**Management**
Initial Assessment	Owner	Advises	None	None	None
Initial Response	Owner	Implements	Updates	Updates	Updates
Collects Forensic Evidence	Implements	Advises	Owner	None	None
Implements Temporary Fix	Owner	Implements	Updates	Updates	Advises
Sends Communication	Advises	Advises	Advises	Implements	Owner
Check with Local Law Enforcement	Updates	Updates	Implements	Updates	Owner
Implements Permanent Fix	Owner	Implements	Updates	Updates	Updates
Determines Financial Impact on Business	Updates	Updates	Advises	Updates	Owner

Document Control

Document Name:	Security Incident Response Plan
Current Version:	
Plan Owner:	
Plan Approver:	
Date of Last Review:	

APPENDIX A

THREAT CLASSIFICATION

The CIA Triad (Confidentiality, Integrity, and Availability) is a framework for incident classification that helps to prioritize the level of incident response required for a cyberattack.

1. **Confidentiality** – Incidents involving unauthorized access to systems, including privileged account compromise. The more confidential the data or the more important the systems are to the business, the higher the potential impact.
2. **Integrity** – Incidents involving data poisoning, including leveraging a privileged account to corrupt or modify data. The more sensitive the data, the higher the potential impact.
3. **Availability** – Incidents that impact the availability or proper functioning of services, such as Distributed Denial of Service (DDoS) or ransomware, including use of privileged accounts to make unauthorized changes. The more critical the services to the business, the higher the potential impact.

When ranking the level of risk to the organization and the type of incident response required, you must consider the extent to which privileged accounts are compromised, including those associated with business users, network administrators, and service or application accounts. When privileged accounts are involved in the breach, the level of risk increases exponentially as does the response required.

APPENDIX B
COMPLIANCE AND LEGAL OBLIGATIONS

PIPEDA
FERPA
SOPPA
COPPA
GDPR
34 CFR Part 300