NON DISCLOSURE / DATA PROCESSING AGREEMENT
FOR SERVICES AND FUNCTIONS PROVIDED ON BEHALF OF THE BOE

This agreement ("Agreement") is dated October 1, 2020 between
The Board of Education of the City of New York with an address at 52 Chambers Street, New York, New York 10007 ("BOE") and
HashCore DLT Inc. dba Rover Labs ("Contractor") with an address at 22 Argyle Road, Port Washington, NY 11050

1. Definitions. "Application" as used in Attachment B means software that performs a user-facing function, such as a web application.

"Biometric Record" means a record of one or more measurable biological or behavioral characteristics that can be used to recognize or identify an individual. Examples include fingerprints; retina and iris patterns; voiceprints; DNA sequence; facial characteristics; and handwriting.

"Handle" as used in Attachment B means, in the context of Protected Information, to create, view, modify, store, transmit or delete

"NIST Cybersecurity Framework" means the U.S. Department of Commerce National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity Version 1.1, or any successor thereto.

"Process" or "Processing" means to perform any act, omission or operation on or with respect to data or information, such as accessing, adapting, altering, blocking, collecting, combining, delivering, deleting, destroying, disclosing, disseminating, erasing, generating, learning of, organizing, recording, releasing, retrieving, reviewing, sharing, storing, transmitting, using or otherwise making data or information available.

"Protected Information," as it relates to BOE's current, future and former employees, students, and their family members (together, "Subjects"), includes, but is not limited to (a) personal and family names, and any variation or abbreviation of a name; (b) physical and electronic addresses, telephone or mobile phone numbers, and geolocation; (c) Biometric Records; (d) personal identifiers, such as social security numbers, student identification numbers, staff identification numbers; (e) indirect identifiers, such as date of birth and place of birth; (f) health information relating to any Subject or their contacts; (g) any other information that, alone or in combination, is linked or linkable to a specific Subject that would allow a reasonable person in a school community, who does not have personal knowledge of the Subject or contact or the relevant circumstances, to identify or locate the Subject with reasonable certainty; or (h) information requested by a person who the Contractor or BOE reasonably believes knows the identity of the Subject or contact e to whom the information relates.

"System" as used in Attachment B means any information technology-processing device, including routers, servers, applications, workstations and mobile devices.

2. Confidentiality. In accordance with the Family Educational Rights and Privacy Act and its implementing regulations (respectively 20 U.S.C. 1232g and 34 C.F.R. Part 99 and together, "FERPA"), the Contractor agrees that it is conducting the services described in the Services Description (the "Services"), attached hereto as Attachment A, on behalf of the BOE, and is acting as a "school official" pursuant to 34 C.F.R. 99.31(a)(1)(B). The Contractor agrees to hold and Process the Protected Information in strict confidence, and not to disclose Protected Information to, or otherwise permit the Processing of Protected Information by, any other parties, nor to Process such Protected Information for the benefit of another or for any use or purpose other than for providing the Services. The confidentiality and data security obligations of the Contractor under this Agreement shall survive any termination of this Agreement. The Contractor agrees to conduct the Services in a manner that does not permit the personal identification of Subjects by anyone other than Authorized Users with legitimate interests in the Protected Information. Contractor agrees to not collect any Biometric Records of Subjects as part of the Services, except to the extent documents in Subjects' handwriting (for example, on consent forms) are provided to or collected by Contractor.

3. Authorized Users. The Contractor shall only disclose Protected Information to its employees (hereinafter referred to as "Personnel"), and its nonemployee agents, assignees, consultants or subcontractors (hereinafter collectively referred to as "Non-Employee Contractors," and together with Personnel, "Authorized Users") who need to Process the Protected Information in order to carry out the Services and in those instances only to the extent justifiable by that need. The Contractor shall ensure that all such Authorized Users comply with the terms of this Agreement. The Contractor agrees that upon request by the BOE, it will provide the BOE with the names and affiliations of the Non-Employee Contractors to whom it proposes to disclose, or has disclosed, Protected Information. The Contractor agrees and acknowledges that the data protection obligations imposed on it by state and federal law, as well as the terms of this Agreement, shall apply to any Non-Employee Contractor it engages to Process Protected Information of the BOE. The Contractor therefore The Contractor agrees to ensure that each Non-Employee Contractor is contractually bound by an agreement that includes confidentiality and data security obligations equivalent to, and no less protective than, those found in this Agreement. Contractor agrees and acknowledges that the data protection obligations imposed on it by state and federal law, as well as the terms of this Agreement shall apply to any Subcontractor it engages in providing the Services to the BOE.

4. Compliance with Law.

(a) The Contractor agrees to hold all Protected Information it Processes in compliance with all applicable provisions of federal, state and local law, including but not limited to FERPA and New York Education Law §2-d and any applicable regulations promulgated thereunder. The Contractor understands that the disclosure of Protected Information to persons or agencies not authorized to receive it is a violation of United States federal law and New York state law, which may result in civil and/or criminal penalties under New York State and Federal laws.

(b) In the event that disclosure of Protected Information (including Protected Information) is required of the Contractor under the provision of any law, judicial order or lawfully-issued subpoena, the Contractor will (a) promptly notify the BOE of the obligations to make such disclosure sufficiently in advance of the disclosure, if possible, to allow the BOE to seek a protective order or to make any notifications required by law, and (b) disclose such Protected Information only to the extent (i) allowed under a protective order, if any, or (ii) necessary to comply with the law or court order. Notwithstanding the foregoing, the BOE acknowledges that the Contractor is required under applicable federal and state law to report certain laboratory testing results, and shall not be required to notify BOE of any such mandatory reporting.

5. Mandatory N.Y. Education Law 2-d Requirements.

(a) BOE Data Privacy and Security Policies. Contractor agrees that it will comply with the BOE's data privacy and security policies, including but not limited to New York City Department of Education Chancellor's Regulation A-820, and any successor thereto.

(b) Subject Data Requests. If permitted by law, the Contractor agrees to notify the BOE of any requests it receives from Subjects or parties authorized by Subjects to amend, inspect, obtain copies of, or otherwise access Protected Information of such Subject in the possession or control of the Contractor, in advance of compliance with such requests. The Contractor shall defer to the judgment of the BOE in granting or denying such requests, and in confirming the identity of Subjects and the validity of any authorizations submitted to the Contractor. The Contractor agrees to assist the BOE in processing such requests in a timely manner, whether received by the Contractor or by the BOE. The Contractor shall amend any Protected Information in accordance with the BOE's decision and direction. Notwithstanding the foregoing, the Contractor shall not be required to notify the BOE if a Subject requests his or her laboratory testing records, and the BOE acknowledges that the Contractor is required under federal and state law to promptly provide such records to a requesting Subject.

(c) Training. The Contractor shall ensure that all Authorized Users with access to the Protected Information are trained, prior to receiving such access and thereafter on a periodic basis, in their confidentiality and data security responsibilities under applicable law and understand the privacy and data security obligations of this Agreement.

(d) Privacy and Security Plan; Additional Data Privacy and Security Protections. The Contractor shall neither retain nor incorporate any of the Protected Information into any database or any medium other than as may be required for it to provide the Services and as required under applicable federal and state law and regulations as well as laboratory accreditation and certification requirements. Contractor agrees to maintain appropriate administrative, technical and physical safeguards in accordance with industry best practices and applicable law to protect the security, confidentiality and integrity of Protected Information in its custody. Contractor agrees to adhere to its data privacy and security plan and the BOE Information Security Requirements (together, the "Plan"), attached hereto as Attachment B. Contractor warrants and represents that (i) its technologies, safeguards and practices, as outlined in the Plan, align with the NIST Cybersecurity Framework, and include sufficient (A) data privacy protections, including processes to ensure that personally identifiable information is not included in public reports or other public documents; and (B) data security protections, including data systems monitoring, encryption of data in motion and at rest, an incident response plan, limitations on access to Protected Information, safeguards to ensure Protected Information is not accessed by unauthorized persons when transmitted over communication networks, and destruction of Protected Information when no longer needed; and (ii) that its Plan meets all additional requirements of New York Education Law 2-d. The Contractor agrees to use encryption technology to protect Protected Information both (i) while in motion or in transit and (ii) while stored, at rest or otherwise in its custody from unauthorized Processing using a technology or methodology specified by the United States Department of Health and Human services in guidance issued under Section 13402(H)(2) of Public Law 111-5. The Contractor acknowledges and agrees to conduct digital and physical periodic risk assessments and to remediate any identified security and privacy vulnerabilities in a timely manner. The BOE reserves the right to request information from Contractor regarding its security practices and compliance with the Plan, prior to authorizing any exchange of Protected Information. The BOE reserves the right to work with the Contractor to develop a risk mitigation plan to resolve any deficiencies in its compliance with the Plan. The BOE reserves the right to promptly terminate the Agreement with no further liability to the Contractor, in the event that the Contractor fails to comply with such risk mitigation plan or is unable to resolve its noncompliance with the Plan. The BOE may audit the Contractor's Processing of the Protected Information for data privacy and data security purposes.

(e) Parent Bill of Rights. The Contractor agrees to comply with the BOE Parents' Bill of Rights for Data Privacy and Security, attached hereto as Attachment C. The Contractor shall complete the Supplemental Information section of Attachment C, and append it to this Agreement. The Contractor acknowledges and agrees that the BOE shall make Contractor's Supplemental Information public, including but not limited to posting it on the BOE's website.

(f) Reportable Data Events. The Contractor shall promptly notify, without unreasonable delay, the BOE Office of Legal Services at 212-374-6888 and at AskLegal@schools.nyc.gov (to the attention of the Chief Privacy Officer) of any act, error or omission, negligence, misconduct, or breach (including any unauthorized release, use or disclosure of, access to Protected Information, whether by the Recipient, its Authorized Users or any other party that shall have gained access to the affected Protected Information) that compromises or is suspected to compromise the security, confidentiality, availability or integrity of Protected Information, including by compromising the physical, technical, administrative or organizational safeguards implemented by the Recipient ("Reportable Data Event"). In no event shall such notification occur more than seventy-two (72) hours after confirmation that a Reportable Data Event occurred. Moreover, to the extent (a) New York Education Law 2-d or any other law or regulation requires parties affected by the Reportable Data Event to be notified, and (b) the Reportable Data Event is not attributable to the acts or omissions of the BOE, the Contractor shall compensate the BOE for the full cost of any notifications that the BOE is required by law to make. Contractor agrees to assist and collaborate with the BOE in ensuring that required notifications shall be clear, concise, use language that is plain and easy to understand, and to the extent available, include: (a) a brief description of the Reportable Data Event, the dates of the incident and the date of discovery, if known; (b) a description of the types of Protected Information affected; (c) an estimate of the number of records affected; (d) a brief description of the investigation or plan to investigate; and (e) contact information for representatives who can assist parents or adult students that have additional questions. The Contractor shall provide any records or other information the BOE requires to investigate the incident or to effectuate the notifications. The Contractor shall fully cooperate with and assist the BOE in investigating the Reportable Data Event, including, without limitation, by providing full access to persons or information necessary to determine the scope of the Reportable Data Event, such as all relevant records, logs, files, data reporting, and other materials required to comply with applicable law or as otherwise required by the BOE.

(g) No Sale or Commercial Use. The Contractor agrees that it will not sell Protected Information; use, disclose or otherwise Process Protected Information for purposes of receiving remuneration, whether directly or indirectly; or use, disclose or otherwise Process Protected Information for marketing, commercial or advertising purposes (or facilitate its use, disclosure or other Processing by any other party for such purposes), or to develop, improve or market products or services to students, or permit another party to do so.

6. Right to Termination. The BOE shall have the right at its sole discretion to terminate the Contractor's access to the BOE's Protected Information upon fifteen (15) days written notice to the Contractor. The BOE shall have the right at its sole discretion to terminate the Contractor's access to the BOE's Protected Information immediately upon the Contractor's breach of any confidentiality obligations herein. No claim for damages will be made or allowed to the Contractor because of said termination.

7. Protected Information Retention, Transfer and Destruction. Whenever required by the BOE, and no later than upon termination of this Agreement, except for Protected Information which the Contractor is required to retain under applicable federal or state law and regulation as well as laboratory accreditation and certification requirements, the Contractor shall promptly (a) with respect to physical copies of Protected Information, surrender, or if surrender is not practicable, securely delete or otherwise destroy Protected Information and (b) with respect to digital and electronic Protected Information, securely delete or otherwise destroy Protected Information remaining in the possession of the Contractor and its Authorized Users, (including all hard copies, archived copies, electronic versions or electronic imaging of hard copies of such data). Contractor shall ensure that no copy, summary, or extract of Protected Information are retained on any storage medium whatsoever by Contractor or its Authorized Users, except as otherwise provided in this Agreement. Any and all measures related to the extraction, transmission, deletion, or destruction of Protected Information will be accomplished utilizing an approved, appropriate and secure method of destruction, including shredding, burning or certified/witnessed destruction of physical materials and verified erasure of electronic media. To the extent that the Contractor continues to be in possession of de-identified data, it agrees not to attempt to re-identify de-identified data and not to transfer de-identified data to any party for re-identification. The contractor agrees not to retain any de-identified Biometric Records. The Contractor shall certify, in writing, that all of the foregoing materials have been surrendered or destroyed (as applicable), except as otherwise provided in this Agreement, in accordance with this Agreement via the "Certificate of Records Disposal" form attached to this Agreement as Attachment D. Provider shall dispose of Protected Information when it is no longer needed to carry out the Services, except as otherwise provided in this Agreement, and shall submit the form found in Attachment D upon disposition. The obligations of this agreement shall apply for so long as Contractor maintains, or is responsible for maintaining, any Protected Information.

8. BOE Property. All Protected Information (a) created or collected by the Contractor, or (b) disclosed or transmitted to the Contractor, pursuant to this Agreement, shall remain the exclusive property of the BOE, or (as applicable) the Subjects. All rights, including the intellectual property rights in and to Protected Information contemplated per this Agreement shall remain the exclusive property of the BOE. Any reports or work product may not contain any Protected Information, unless required by the BOE or if necessary to carry out the Services.

9. Other Agreements. The Contractor agrees that to the extent that any confidentiality or data security terms or conditions regarding the Services found in another agreement binding BOE employees, subcontractors, parents or students (together, "BOE Users,") including but not limited to any end-user license agreement, "click wrap," "click-through," "click and accept," "web-wrap," or other form of agreement requiring the individual user to accept terms in order to use or benefit from the Services, conflict with the terms found in this Agreement, the terms and conditions which afford more protection to BOE Users shall apply. Any subsequent agreements between the Contractor and the BOE with respect to the

provision of the Services shall include confidentiality and data security obligations on the part of the Contractor at least as strict as set those forth in this Agreement. In the event a subsequent agreement fails to contain confidentiality and data security provisions with obligations at least as strict as this Agreement, the confidentiality provisions of this Agreement shall be deemed inserted therein, and shall continue to bind the Contractor, unless such subsequent agreement specifically references this Agreement by name and disclaims its obligations in writing.

10. Other Terms.

(a) The Contractor agrees that money damages would be an insufficient remedy for breach or threatened breach of this Agreement by the Contractor. Accordingly, in addition to all other remedies that the BOE may have, the BOE shall be entitled to specific performance and injunctive or other equitable relief as a remedy for any breach of the confidentiality and other obligations of this Agreement.

(b) Nothing in this Agreement obligates either party to consummate a transaction, to enter into any agreement or negotiations with respect thereto, or to take any other action not expressly agreed to herein.

(c) The Contractor shall defend, indemnify and hold harmless the BOE and the City of New York from any and all claims brought by third parties to the extent arising from, or in connection with, any negligent acts or omissions of the Contractor and the Contractor's Authorized Users or any other representatives for whom the Contractor is legally responsible for, in connection with the performance of this Agreement.

(d) No failure or delay (in whole or in part) on the part of either party hereto to exercise any right or remedy hereunder shall impair any such right or remedy, operate as a waiver thereof, or affect any right or remedy hereunder. All rights and remedies hereunder are cumulative and are not exclusive of any other rights or remedies provided hereunder or by law or equity. To the extent any provision of this Agreement is held to be unenforceable or invalid, the remainder of the Agreement shall be remain in full force and effect, and the Agreement shall be interpreted to give effect to the such provision to the maximum extent permitted by law.

(e) This Agreement shall be governed by and construed in accordance with the law of the State of New York. The Federal or State Courts of New York City, New York will have exclusive jurisdiction to adjudicate any dispute arising under or in connection with this Agreement. This Agreement constitutes the entire Agreement with respect to the subject matter hereof; it supersedes any other Contractor terms and conditions, all prior agreements or understandings of the parties, oral or written, relating to the Services and shall not be modified or amended except in writing signed by the Contractor and the BOE. The Contractor may not assign or transfer, without the prior written consent of the BOE, this Agreement. This Agreement shall inure to the benefit of the respective parties, their legal representatives, successors, and permitted assigns. This Agreement is effective upon execution of the Contractor.

Signed and Agreed to:

HashCore DLT Inc. dba Rover Labs

By: ______________________

Date: APR 30, 2021

Name: Mark Fasciano ____________

Title: CEO ______________________

Contractor Acknowledgment

State of New York }
} ss.:
County of ~~New York~~ Nassau }

On this 30th day of April, 2021, before me, the undersigned, a Notary Public in and for said State, personally appeared one ______, personally known to me or proved to me on the basis of satisfactory evidence to be the individual whose name is subscribed to the within instrument and acknowledged to me that he/she executed the same in his/her capacity, and that by his/her signature on the instrument, the entity or individual upon behalf of which the individual acted, executed the instrument. by Mark Fasciano.

Lynn J Moessner NOTARY PUBLIC

LYNN J MOESSNER
Notary Public, State of New York
No. 01M04970982
Qualified in Nassau County
Commission Expires 8/20/2022

Pursuant to Executive order 202.7.

Attachment A: Services Description

Rover will handle end-to-end responsibility for saliva testing including:

- Pre-loading of information received from DOE for consenting test subjects
- Test kit provisioning and shipping to DOE locations
- Training and support of collection supervisors (nurses)
- Management of sample transportation from DOE locations to testing lab
- Processing samples for COVID testing on Advanta Dx platform
- Disposal of samples after testing
- Laboratory info system (LIS) for test registration, lab processing, delivery of results and/or reports to test subjects or parent/guardian, NYC DOE Situation Room, and NYS pandemic tracing
- Third-party penetration test of LIS and ongoing vulnerability monitoring
- Support for test subject/parent/guardian on receiving test results

Attachment B
Section 1

Information Security Requirements For Contractors

Office of Information Security
Division of Instructional and Information Technology
NYC Department of Education

CLASSIFICATION: PUBLIC.

This document may be distributed without restriction.

1. Information Security Policies

A. Contractor must have, and upon request by the DOE shall promptly provide the DOE with copies of its, information security policies that cover the followingelements:

1. Data classification andprivacy
2. Security training andawareness
3. Systems administration, patching and configuration
4. Application development and code review
5. Incident response
6. Workstation management, mobile devices and antivirus
7. Backups, disaster recovery and business continuity
8. Regular audits andtesting
9. Requirements for third-party business partners and contractors
10. Compliance with information security or privacy laws, rules, regulations or standards
11. Any other information security policies

B. Policy Requirements: In addition to addressing the elements set forth above:

1. Contractor must indicate in their policies the date of the most recent revision.
2. Contractor must include a certification from its Chief Operating Officer, or individual with an equivalent title with authority to represent the Contractor, asserting that all of the above elements are addressed in the Contractor's security policies, and that such policies are at least as rigorous as the policies set forth in this document and the NYC Citywide Information Security Policies issued by the NYC Cyber Command, in cooperation with DoITT (Cyber Policies). If Contractor cannot make such certification for any reason (e.g. Contractor's policies do not address an element listed above), Contractor must notify the DOE of the deficiency and explain how Contractor will remedy such deficiency.
3. Contractor shall complywith such policies and, unless the Contractor receives the DOE's prior written approval, Contractor shall not make any changes to such policies that would result in (i) not addressing one or more elements set forth above or (ii) not being as rigorous as the policies set forth in this document or the NYC Cyber Policies.

2. Privacy & Confidentiality

In accordance with the Agreement, Contractor must hold Protected Information in strict confidence and not disclose it to any third parties nor make use of such data for its own benefit or for the benefit of another, or for any use other than the permitted purpose agreed.

A. The Contractor shall use commercially reasonable efforts to secure and defend any system housing Protected Information against third parties who may seek to breach the security thereof, including, but not limited to breaches by unauthorized access or making unauthorized modifications to such System.

B. The Contractor shall protect and secure all Protected Information in transit (collected, copied and moved) and at rest (stored on the physical servers), including during any electronic data transmission or electronic or physical mediatransfer.

C. The Contractor shall maintain all copies or reproductions of Protected Information with the same security it maintains the originals. At the point in which the Protected Information is no longer necessary for its primary or retention purposes, as authorized by DOE, Contractor must destroy such data, making it unusable and unrecoverable. If Contractor determines at such point that destruction of the Protected Information is infeasible, Contractor will provide DOE with a reasonable explanation and will cease any access or use of the Protected Information.

The provisions noted above will not apply to Protected Information which the Contractor is required to retain under applicable federal or state law and regulation as well as laboratory accreditation and certification requirements. However, the Contractor will continue to abide by the confidentiality and data security terms of its agreement with the DOE while it retains Protected Information, or causes it to be retained.

Contractor's at-rest database is encrypted, and public access to Contractor's data systems is secured using industry-standard security and best practices. The retention period will be the greater of seven years or the retention period defined by federal or state regulations.

Protected Information will not be shared to outside entities, except as required by federal or state law.

D. For all Application screens, front pages of any reports and landing pages of web Applications that contain Protected Information, Contractor must include prominent confidentiality notices in legible-sized font on each page (e.g. a prominent notice that the information on such screen or report is confidential on the bottom of a web screen or the footer of a report page).

E. All web Application screens that contain Protected Information must be non-cacheable.

F. Protected Information should not appear in URLs.

G. Contractor's development, test and QA environments shall not use actual Protected Information unless additional safeguards are put into place to protect the confidentiality of the information.

H. Contractor must comply with any additional requirements set forth in its data use agreement, non-disclosure agreement, or any similar contract or agreement with the DOE that is related to the subject matter to which these requirements apply

3. Application Development

A. Where applicable, Contractor shall have a comprehensive secure development lifecycle System in place consistent with industry standard best practices, including policies, training, audits, testing, emergency updates, proactive management, and regular updates to the secure development lifecycle System itself.

B. Code for Applications that handle Confidential Information must comply with the DOE Secure Coding Standard for Contractors. The DOE must approve any exceptions to this standard in writing.

C. Where applicable, Contractor must review and test all application code for security weaknesses and backdoors prior to deployment with DOE. All high-risk findings and exploitable vulnerabilities must be resolved before the Application is released. A development manager of Contractor must certify in writing to the DOE that a security review has been conducted and that all risks are acceptable before every release. For further information, please refer NIST SP 800-160 Volume 1 (System Life Cycle Processes and Systems Security Engineering) and SP 800-37 Rev. 2 (Risk Management Framework).

D. Contractors that handle Protected Information must respond to and resolve security-related reports, inquiries and incidents in a timely and professional manner. The Contractor must notify the DOE within 24 hours of when Contractor becomes aware of any such incident or suspected incident that poses a potential risk to the Protected Information. The Contractor shall send the notification to appsecurity@schools.nyc.gov and to studentprivacy@schools.nyc.gov.

4. Authentication & Identity Management

A. If an application requires Single Sign-On (SSO) integration with the DOE, the Contractor must support authentication for DOE Users as specified in the DIIT SAML Integration Guidelines

1. Contractor will not have the ability to make any changes to the DOE Identity Management Systems.
2. If new DOE Users need to be enrolled or registered in order to use a Contractor's System, The NYCDOE Office of Information Security must receive and agree upon the plan for the registration process and ownership of identity management in writing.
3. Follow DIIT OpenId and SAML Integration guidelines if application requires Single Sign-on.

B. If the Contractor maintains its own identity management system for its users, it must:

1. Enforce a one user, one account policy in which shared/ group accounts and duplicate accounts are not permitted
2. Be free of testing, development and non-production accounts.
3. Maintain accurate legal name, address, phone number information for all users who are permitted to access Protected Information, and upon request from the DOE, produce lists of users who will have access to Protected Information.
4. Enforce a strong password policy of eight characters minimum, with mixed case and at least one number

or special character.

5. Store all passwords in non-reversible one-way cryptographic hash.
6. Log all successful and failed authentication attempts, including date, time, IP address, and username.
7. Offer a secure password reset feature, including verification of identity, email or text notification and a one-time-use password link that expires after 24 hours.
8. Automatically de-provision accounts for terminated employees of Contractor and DOE.
9. Temporarily lock accounts with repeated failed login attempts and provide support to affected users.
10. Keep attributes and group structures that support authorization accurate.
11. Don't hardcode credentials
12. Use a password Reset Tool whenever possible
13. Implement account lockout against brute-force attacks
14. Don't disclose too much information in error messages
15. Store database credentials securely
16. Encrypt credentials in transit
17. Password must expire in 90 days
18. Applications that use non-standard authentication solutions require approval from Office of Information Security

5. Protected Information Authorization

A. Applications that handle Protected Information must have explicitly defined authorization controls that prevent users from exceeding their authorized privileges.

B. Any applications must perform authorization checks before performing any action that creates, views, updates, provides access to, transmits or deletes Protected Information. Authorization logic must be highly configurable.

C. Authorization checks must verify the user is authorized to perform the requested action, including the scope of the action. Scope authorization checks should reference DOE location codes, student-teacher-class linkage, parent-student linkage and other data sources.

D. Whenever possible, authorization checks will use the DOE RBAC framework, DOE identity management system and other DOE Systems of record. Access to these Systems may be via a web service or replicated database, at the DOE's discretion. The Contractor Application will not be able to make any changes to the contents of these Systems.

E. Any non-DOE accounts that are managed locally by the Contractor must follow the principal of "Least Privileged Access" whereby those user accounts are provided the most restrictive access necessary to perform the required business function. "Super users" (i.e. application administrators) must be avoided unless absolutely necessary due to a legitimate administrative or educational need for such access in order to provide the Services.

6. Incident Response

A. Contractor must have a plan for compliance with all applicable breach notification laws, including but not limited to New York State Education Law § 2-d and the New York State Data Breach Notification Act (General Business Law §899-aa and New York State Technology Law § 208, as appropriate).

B. The DOE must be notified in writing within 24 hours of the earliest indication or report of a potential breach or unintended disclosure of Protected Information or a system that supports it.

C. Response actions to incidents that might affect Protected Information or systems must be conducted quickly and with ample resources. Contractor will hire a professional third-party incident response team if in- house resources do not have sufficient skill or availability.

D. DOE shall have the right to view all incident response evidence, reports, communications and related materials upon request.

E. If requested by the DOE, or if required by law, the Contractor shall notify in writing all persons affected by the incident, at its own cost and expense, or shall compensate the DOE for the cost and expense of notifications it makes.

F. Contractor's IT security program includes a security incident response policy and procedure. The incident response procedure defines incident types, risk levels, step by step procedure for responding to each event type, contact personnel, management, internal and external communication procedures, local law enforcement agency information, etc.

7. Audit & Inspection

A. The Contractor shall allow DOE, upon reasonable notice, to perform security assessments or audits of Systems that handle or support Protected Information related to the subject matter to which these requirements apply. Such an assessment shall be conducted by an independent 3rd party agreed upon by the Contractor and the DOE, and at the DOE's own expense, *provided* that the Contractor cooperate with any such assessment/audit and shall, at its own expense, provide all necessary support, personnel and information needed to ensure the successful completion of the assessments or audits.

B. The Contractor shall provide DOE, upon DOE's request, with a SSAE 16 or similar report as agreed to by DOE for critical business processes relating to protection of Protected Information and safeguards implemented in its organization.

C. Contractor must engage an independent third party annually to assess the practical security of Contractor's Systems. These reviews must include penetration tests from the perspective of an external attacker and an internal user with common privileges. The penetration tests must include all Systems exposed to the internet and any Systems, internal or external, that Handle Protected Information. Such annual assessment shall be at Contractor's sole expense.

D. Any Contractor housing Protected Information must have for the duration of the contract an independent third-party Contractor specializing in continuous monitoring and reporting on Information Security events. The reports and or electronic access must be made available to DOE Information Security personnel at any time.

E. Audit logs must be implemented for all systems that handle Protected Information. All attempted violations of system security must generate an audit log. Audit logs must be secured against unauthorized access or modification.

F. In the event of adverse findings through a DOE or Contractor audit, the Contractor shall cooperate with the DOE in remediating any risks to Protected Information, including complying with request to temporarily taking the system offline or otherwise limiting access to the system, and any other follow up actions reasonably necessary to secure the Protected Information.

8. Availability

A. Contractor Systems that handle Protected Information shall be available and fully functional 24x7x365 with 99.9% uptime, unless otherwise agreed upon in writing with the DOE. Contractor shall make plans for colocation, backups and any other systems necessary to ensure continuity.

B. Contractor must notify and obtain agreement from the DOE for any planned interruptions in service related to the agreement to which these requirements apply, with the exception of emergency security updates. Contractor must notify the DOE immediately of any unintended service interruption.

C. In order to maintain performance and security of the Services, Rover Labs will perform scheduled maintenance within its published maintenance windows. This may require specific Services to be suspended during the maintenance period. Loss of Service Availability due to scheduled maintenance will not be included in the calculation of Service Availability. Rover Labs will use commercially reasonable efforts to notify the DOE in advance of any scheduled maintenance that may adversely affect Services.

9. Encryption

A. All systems that handle Protected Information must encrypt the DOE data that include Protected Information in transit in a manner consistent with the most recent NIST guidelines.

B. For HTTP and other protocols that use SSL/TLS, Contractor shall use the TLS 1.2 or later protocol with 128-bit or larger key size, and shall make previous protocols and smaller keys unavailable.

C. Contractor shall utilize a third party provider that is a recognized and trusted authority in the industry to generate any certificates that are used for authentication between two parties (e.g., Contractor and the DOE or Contractor and any other party).

D. Web Applications that contain Protected Information must be available only over Transport Layer Security ("TLS"). Attempts to use the Application without encryption shall be rejected. Encrypted and non-encrypted content shall not be mixed.

E. Data at rest that is stored outside of hardened Application or database production Systems must be protected by encryption consistent with NIST recommendations.

F. The Contractor shall keep private keys confidential, implement key lifecycle management and protect all keys in storage or in transit.

G. The Contractor shall choose keys randomly from the entire key space and ensure that encryption keys allow for retrieval for administrative or forensic use.

H. Encryption of the DOE data in production databases is *not* required. Any database encryption system must be approved by the DOE, which approval shall not be unreasonably withheld. All DOE data must be recoverable. Contractor agrees to deliver decrypted data requests within 72 hours.

I. Contractor will not store DOE data outside of the United States. In the event that Contractor will store DOE data outside of the United States at a later date, Contractor shall notify the DOE of the locations outside the U.S. by providing notice either in its contract or proposal to a RFP/RFB if known by Contractor prior to award, or if known after award, to studentprivacy@schools.nyc.gov; *provided* that the DOE reserves the right to require that the use, storage, or handling of DOE data occur within the contiguous United States or similar regional boundary as defined by the DOE, which, if applicable, shall be specified in the contract or RFP/RFB.

J. Disable HTTP access for all SSL enabled resources

K. Use the Strict-Transport-Security header

L. Store user passwords using a strong, iterative, salted hash

M. Securely exchange encryption keys

N. Setup a secure key management processes

O. Disable weak SSL ciphers on servers

P. Use valid SSL certificates from a reputable CA

Q. Disable data caching using cache control headers and autocomplete

R. Limit the use and storage of sensitive data.

10. Data retention/destruction

A. Contractor may be required to support retention of Protected Information as per New York State Retention Schedule LGS-1.

B. If applicable, retention requirements for DOE data may be specified in a contract or RFP/RFB. If applicable, the Contractor must acknowledge in its proposal to a RFP/RFB that it can meet the requirements and, upon request by the DOE, demonstrate that retention requirements are implemented.

C. Record retention systems must comply with all security and privacy controls set forth in this document.

D. Whenever required by the BOE, and upon termination of this agreement, and except as noted below, the Contractor will promptly (a) with respect to physical copies of Protected Information, surrender, or if surrender is not practicable, securely delete or otherwise destroy Protected Information and (b) with respect to digital and electronic Protected Information, securely delete or otherwise destroy Protected Information remaining in the possession of the Contractor. This will include all hard copies, archived copies, electronic versions or electronic imaging of hard copies of such data. The Contractor will ensure that no copy, summary, or extract of Protected Information is retained on any storage medium whatsoever by Contractor, except as noted below. Contractor will accomplish all measures related to the extraction, transmission, deletion, or destruction of Protected Information utilizing an approved, appropriate and secure method of destruction. This may include shredding, burning or certified/witnessed destruction of physical materials and verified erasure of electronic media. To the extent that the Contractor continues to be in possession of de-identified data, it will not to attempt to re-identify de-identified data and not to transfer de-identified data to any party for re-identification. The Contractor will not to retain any de-identified biometric records. The Contractor will certify, in writing, that all of the foregoing materials have been surrendered or destroyed (as applicable), except as noted below.

E. The provisions noted in section D above will not apply to Protected Information which the Contractor is required to retain under applicable federal or state law and regulation as well as laboratory accreditation and certification requirements. However, the Contractor will continue to abide by the confidentiality and data security terms of its agreement with the DOE while it retains Protected Information, or causes it to be retained.

11. System Configuration & Maintenance

A. All operating systems, servers, and network devices that support DOE systems or Protected Information must be kept hardenedand patched.

B. All Contractor systems that are used to host, transfer, or otherwise interact with Protected Information must enforce strict separation from any non-DOE systems. This may be achieved through physical and/or logical separation. The separation must be auditable and able to be proven at the request of the DOE.

C. Contractor must maintain technical best security practices configuration guidelines for all such systems and update them at least twice per year.

D. All security-related patches must be installed on systems within a reasonable timeframe. Contractor will maintain a testing lab in order to support this.

E. Establish a rigorous change management process

F. Define security requirements

G. Conduct a design review

H. Perform code reviews

I. Perform security testing

J. Harden the infrastructure

K. Define an incident handling plan

L. Keep browser updated with latest version.

12. Subcontractors

A. Contractor has represented that it will not utilize sub-contractors to perform testing, but may use a third party to assist with Help Desk customer service. However, should it do so, in addition to the subcontracting provisions in the agreement with the DOE (which require DOE approval of all subcontractors), in the event that a Contractor utilizes subcontractors to support a system that handles Protected Information (each a "subcontractor"), such subcontractors shall be subject to, and Contractor must require that each subcontractor comply with, the requirements set forth herein.

13. New York City Parents' Bill of Rights for Data Privacy and Security ("PBOR")

A. Contractor shall comply with the requirements of the PBOR in every respect. As detailed in its agreement with the DOE, it will not sell Protected Information or release it for any commercial purposes. It will facilitate the parents' right to inspect and review their children's Protected Information in the custody of the Contractor. As detailed in the previous sections of this document, it shall maintain safeguards to protect Protected Information when it is stored or transferred, and represents that these safeguards meet industry standards and best practices. Contractor shall respond appropriately to complaints parents make about possible breaches of Protected Information. It has agreed to the DOE's full PBOR as part of this agreement and provided the supplemental information required of it for public posting on the DOE's website, pursuant to New York Education Law 2-d.

14. Training

Employees go through a background check as well as drug screening prior to employment. New hires go through an orientation program where employees are educated on federal and state laws governing confidentiality and security of healthcare data. On an ongoing basis, compliance and security awareness events are conducted for employee education and awareness.

15. Appendix (A) – DIIT SAML Integration Guidelines

"SAML" – means Security Assertion Markup Language

SAML allows Single Sign-On between Partner Websites and through this allowing sharing of user identities to provide a better user experience. SAML can thus be used for:

- Web Single Sign-On (SSO)
- Attribute-based Authorization (followed by Web SSO)
- Securing Web Services

SAML Components

Below is a list of some SAML components included for the purpose of this document:

Assertion

An assertion is a package of information that supplies one or more statements made by a SAML authority (the Identity Provider). The assertion may contain authentication information, attributes for authorization and other information as desired.

Identity Provider

The Identity Provider (or IdP) is the user authenticating authority in a SAML environment, responsible for authenticating a user and providing authorization information. DOE will assume this role.

Service Provider

The Service Provider (or SP) is the partner or service that requests for and consumes the user authentication and authorization information, enabling users to access their Website or Web Services without re-authenticating themselves. The content provider will assume this role.

Protocols

Defines a number of requests/response protocols that allow service providers to:

- Request from SAML authority one or more assertions.
- Request that an IDP authenticate a principal and return the corresponding assertion.
- Request that a name identifier be registered.
- Request that the use of an identifier be terminated.
- Retrieve a protocol message that has been requested by means of an artifact.
- Request a near-simultaneous logout of a collection of related sessions (Single Logout)
- Request a name identifier mapping.

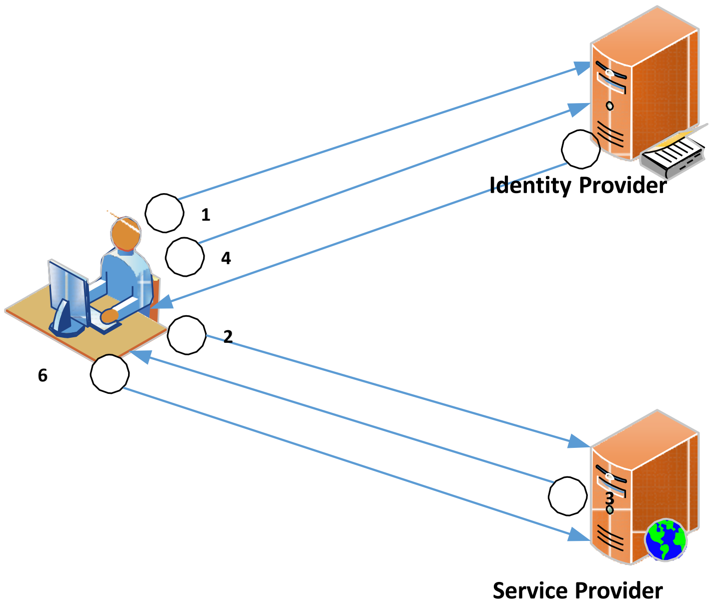
Binding

Defines how the IdP and SP exchange information. The most common bindings are:

- HTTP Redirect (GET) Binding
- HTTP POST Binding
- HTTP Artifact Binding

SAML Flow

The following diagram illustrates the SAML flow from a high-level for the SAML Post Binding with an Identity Provider initiated login.



1. User logins to an SSO Portal (Identity Provider -IdP)
2. User then clicks on a Partner website link (Service Provider- SP)
3. The SP then asks the IdP to authenticate the user sending a signed authentication request.
4. The request is redirected through the user browser to the IdP.
5. The IdP validates the request and sends a signed SAML assertion back (the user would have been challenged for credentials by the IdP if he/she hadn't already logged in).
6. The SAML assertion is redirected to the SP through the user browser. The SP identifies and authorizes the user using information in the assertion and logs in the user

Note: For security, purposes it is optimal that all communication occurs over a secure channel (HTTPS) and all information be digitally signed by either party.

Attachment B
Section 2

Doe Secure Coding Standard For Contractors

Office of Information Security

Division of Instructional and Information Technology

NYC Department of Education

CLASSIFICATION: PUBLIC.

This document may be distributed without restriction.

Secure Coding

The terms Non-public, Restricted, Sensitive, and Public are defined in the *Data Classification Standard*, which can be referenced DOITT Citywide Information Security Policies & DOE Information Security Requirements. For purposes of this document, the term "Confidential Information" defined in Section 3 of the DOE Information Security Requirements means "Restricted" and "Sensitive" information as defined in the Data Classification Standard. The term "Non-public Information" includes Confidential Information, Restricted Information and Sensitive Information.

Privacy Guidelines

Privacy features should be clearly defined. When you begin working on a project, think about what Non-public information it handles, how many users have access to it, and where it will be accessible from. You should be clear on what users have which roles, what tasks a role may perform, and what data a given user may access.

Think critically about privacy. If the security controls are not clearly defined, or do not seem adequate for the level of risk, please inquire the Office of Information Security.

- **Keep use of Non-public Information to a minimum.** Do not disclose Non-public data to users that is not explicitly required in the application's specification.
- **Confidential Information should be masked whenever possible.** When working with data that has a Non-public classification, such as social security numbers or passwords, mask the data whenever possible. For example, only display the last four digits of a SSN unless there is a specific need for the entire number.
- **Limit the use of Non-public information on grid screens.** Do not include Non-public Information on grid screens unless it is essential. Keep them on single record detail screens where their use can be logged more carefully, and fewer records can inadvertently be disclosed.
- **Pages with Non-public Information should not be cached.** Any page that contains Non-public information should be served with headers explicitly instructing the browser not to cache it.
- **Non-public Information should not be transmitted in GET query data.** Non-public Information should never be transmitted in GET query strings of HTTP requests. URL and query strings are often logged by browsers, proxy servers, etc…
- **Unauthorized data should not be "hidden" on the client.** Assume that the user can view any data that has been transmitted. HTML comments, "Hidden" form fields; ViewState, etc… are insecure and should not be used to protect Non-public Information. Do not send any information that the user may not have appropriate permissions to view.
- **Bulk data transfers must have strong security features and be approved by DOE Information Security.** In general, Non-public data should not be downloadable in bulk, or transmitted to any third parties. When bulk transfers or downloads is necessary, security controls must be in place. The dataset should be as limited as possible. Transfers or downloads must generate audit logs, have transmission encryption, and the receiving parties must be authenticated and authorized.
- Any transfers of data to third parties must be approved by DIIT prior to implementation.

Authentication

- **Require authentication.** Any application features or data that should not be publicly and anonymously accessible must require username/password authentication.
- **Central Active Directory (CAD).** Most web applications should use CAD as their authentication source. Do not create application-specific authentication sources in SQL databases, text files or other places. Exceptions must be approved by the Office of Information Security prior to development.
- **Federation.** Applications that are hosted by third parties should use Federation via SAML or ADFS for authentication. Federated authentication is useful when a trusted third party maintains its own identity database, or needs to authorize DOE users for its applications. If your project requires Federation, please speak with the Office of Information Security.
- **Shared accounts are forbidden.** Authentication must identify a unique person. It is never acceptable for people, vendors or other agencies to share accounts or have a "group" account. (Exceptions may be made for data services between applications.)

- **Encrypt credentials in transit.** Credentials such as usernames, passwords and session identifiers should always be encrypted in transit. Passwords should never be sent in the same communication with a username/userID.

Requirements for non-standard authentication solutions:

- **Password storage.** Passwords must never be stored in plaintext. Store user passwords using a strong, iterative cryptographically salted and hashed values.
- **Password complexity.** Passwords must be complex in character content and length—at least eight characters, mixed case, with at least one number and one punctuation character.
- **Expiration.** Passwords must expire after 90 days.
- **Lockouts.** Accounts should be locked for 30 minutes after five unsuccessful login attempts.
- **Resets.** Password resets should use a one-time link. The link should be mailed to the user's pre-registered email address, and remain active for no longer than 24 hours. The reset process should allow the user to enter a new password. Passwords should never be sent in the same communication with a username/userID.
- **Accountability.** Failed login attempts, account lockouts, password reset requests, account enrollment and deletion, and the last successful login must be logged.
- Follow the DIIT OpenId and SAML Integration guidelines if application required Single Sign-on.

Session state:

- **Use platform-supplied state mechanism.** Do not create custom session-state solutions. Use the platform's built-in session management.
- **Timeouts must be reasonable.** Users should be automatically logged out after 15 minutes of inactivity if an application uses Private or Confidential data, and 30 minutes maximum for any application.
- **Session identifiers must be encrypted in transit.** Session IDs should never be transmitted in plaintext. When cookies are issued, ensure that the "secure" option is set, which instructs the browser to never transmit it without encryption.
- **Require logout feature for forms applications.** If an application uses forms-based authentications, as opposed to NT integrated authentication, users must be given a logout button to end their session.
- **Ensure that session identifiers are sufficiently random.** Session token must be generated by secure random functions and must be of sufficient length to withstand analysis and prediction.
- **Regenerate session tokens.** Session tokens should be regenerated when the user authenticates to the application and when the user privilege level changes.
- **Implement an absolute session timeout.** Users should be logged out after an extensive amount of time (e.g. 4-8 hours) has passed since they logged in.
- **Destroy sessions at any sign of tampering.** Unless the application requires multiple simultaneous sessions for a single user, implement features to detect session cloning attempts. Should any sign of session cloning be detected, the session should be destroyed, forcing the real user to re-authenticate.
- **Use secure cookie attributes (i.e. HTTP Only and Secure flags).** The session cookie should be set with both the HttpOnly and the secure flags. This ensures that the session id will not be accessible to client-side scripts and it will only be transmitted over HTTPS, respectively.
- Set the cookie domain and path correctly
- **Set the cookie expiration time.** The session cookie should have a reasonable expiration time. Non-expiring session cookies should be avoided.

Authorization

- **Require authorization for application access.** After authentication, the application should verify that the user has an appropriate role to use it. Applications should not be accessible to the entire population of authenticated users. For instance, an application intended to be used exclusively by principals should ensure that teachers cannot access it.
- **Authorize features and operations.** The application should support granular per-operation authorization controls. Permission should be verified before performing Create, Read, Update and/or Delete (CRUD) operations or other

important tasks.

- **Authorize scope.** The application should support scope-based authorization controls. Permission should be verified before accessing or manipulating a data record. For instance, if a principal is attempting to access a student's grades, the application should verify that the student is in his or her school.
- **Make authorization configurable.** It should not be necessary to re-code, compile or deploy an application in order to change authorization logic. Authorization Module methods such as IsAuthorizedForTask and GetLocations make this simple.
- **Authorization failures.** Authorization failures should throw an exception, generate a log event, and display a generic error message to the user.
- **Comment authorization needs.** Authorization needs and explanations should be clearly commented in code.
- **Apply access control checks consistently.** Always apply the principle of complete mediation, forcing all requests through a common security "gate keeper." This ensures that access control checks are triggered whether or not the user is authenticated.
- **Apply the principle of least privilege.** All access decisions should be based on the principle of least privilege. If not explicitly allowed then access should be denied.
- **Don't use direct object references for access control checks.** Do not allow direct references to files or parameters that can be manipulated to grant excessive access. Access control decisions must be based on the authenticated user identify and trusted server side information.
- **Don't use un-validated forwards or redirects.** An unvalidated forward can allow an attacker to access private content without authentication. Unvalidated redirects allow an attacker to lure victims into visiting malicious sites. Prevent these from occurring by conducting the appropriate access controls checks before sending the user to the given location.

Accountability

- Privacy features should be clearly defined
- Keep Non-public Information to a minimum
- Confidential information should be masked whenever possible
- Pages with Non-Public Information should not be cached
- Non-public Information should not be transmitted in GET query data
- Unauthorized data should not be "hidden" on the client.
- Require logging for accountability and privacy
- Information classification labelling must be used
- **Require logging for accountability and privacy.** Applications must generate logs for the purposes of accountability and privacy, not just debugging and troubleshooting.
- **Information classification labelling.** Applications, reports and documents that contain non-public information should always be cleared labeled as per the Data Classification Standard. Reports should always include the name of the user that generated them and the date.

Operations That Require Logging

- **Operations on Non-public Data.** The creation, retrieval, modification or deletion of Non-public data must be carefully tracked.
- **Authentication events.** Failed login attempts, password reset requests, lockouts, user creation / enrollment / deletion and the last successful login should always be logged. (If you are using DOE Federation or Active Directory as an authentication source, you do not need to manually implement this.)
- **Authorization failures.** Any authorization check that fails must be logged.
- **Information to include in log entries.** Log entries should include the date, time, username, IP address, and description of the event being logged.

Input Validation

- **Require input validation.** All user- and client-supplied input must be validated before use. This includes data being transmitted in headers, cookies, URL query data, POST form data, hidden form fields, and web service calls. All data is "guilty" until proven innocent.
- **Validation must occur on the server.** Browser-based validation may be useful as an interface feature, but is not effective for security purposes.
- **Reusable modules should include validation.** Any re-usable code component should perform its own validation, even if it may be redundant in some cases. For instance, a modular data-layer helper should always perform validation, because it may be re-used in an application where the web pages do not.
- **"White list" criteria.** Data should always be validated for length and character content using "white list" logic. Specifically permit what is appropriate, and deny anything else by default. Never include non-printable characters, SQL syntax markers, etc. unless there is a good reason.

For instance, if you are expecting a phone number, validate that the value is no more than 16 characters long and only comprised of digits, hyphens, spaces and parentheses.

- **Transformations.** In some cases where punctuation or unusual characters are necessary, transform them into HTML entities, such as turning a single quote into "&quot;"
- **Use Validator tags and Regular Expressions.** Every form field should have a server-side regular expression validator. For input that does not come from a form field, in-line regular expressions tests are the preferred method for input validation.
- **Validation failures.** In general, when input validation fails, the application should stop processing the request and display an error. Only "mend" user data for minor predictable issues, such as removing dashes from a phone number.
- **Comment complex validation needs.** Regular expressions can be difficult to read quickly. Comment any input validation logic that is not immediately intuitive.
- **The use of unmanaged code is prohibited.** Using unmanaged code can introduce buffer overflow vulnerabilities. If a project must use unmanaged code, please speak with the Office of Information Security.
- Conduct contextual output encoding
- Use tokens to prevent forged requests
- Set encoding for your application
- Use the no sniff header for uploaded content
- Use the X-Frame-Options header
- Use Content Security Policy(CSP) or X-XSS-Protection headers

Output Validation

- **Perform output validation.** Many attacks such as cross-site scripting, drive-by downloads and browser exploitation work by feeding malicious data to web applications for display or distribution.
- Be careful when assembling content that uses client-supplied data. Beware of overly long strings, less-than, greater-than, semicolon, parentheses, single quote, double quotes and other HTML and Javascript syntax tokens.
- **Use ASP.Net validation features, white-list regular expressions and encoding.** Normally, ASP.Net will prevent potentially hazardous characters from "breaking out" of form fields, labels and other display controls. However, if you are "manually" generating HTML or Javascript, you need to do this yourself.
- You can use HttpUtility.HTMLEncode to transform non-alphanumeric characters into HTML-safe entities. Use regular expressions to do general sanity checks for character length and content.
- **Require output validation for email.** Carefully validate all data that is used in email messages. Remember that most popular mail clients are either web applications or use embedded web browser controls to display messages.

Database Access

- **String-building is forbidden.** An application should never piece together SQL statements from strings. This creates the risk of SQL injection. Note that string-building can occur inside stored procedures that use EXEC. **Use stored procedures whenever possible.** Stored procedures save the structure of the SQL query on the database. This is the best way to prevent SQL injection. It also offers advantages for organization, performance and granular authorization.
- **If stored procedures are not possible, use prepared statements.** Prepared statements safely separate SQL queries and parameter values. This effectively prevents SQL injection, but does not offer the other advantages of stored procedures.
- **Each application must have its own database account.** Applications may not share database accounts. Each account's permissions should be tightly configured so that it can only access the appropriate databases, tables and procedures.
- **Use stored procedures whenever possible**

File Access

- **File paths should be built with extreme caution.** If any client-supplied input is used to construct a file name or path, use strong input validation. Beware of slashes, backslashes and periods. It should never be possible escape the intended directory. Validate using "white list" logic.
- **Store data and report files outside the webroot.** Do not allow users to directly request files for download or view filesystem directories. Have the application act as an intermediary. Data, report and other files for download or reference should always be stored outside of the webroot.
- **Explicitly set permissions on created or uploaded files and directories.** In general, files should be set read- only, and only by the web server's user. Never allow a file to be created with any execute or world-write permissions.
- **Validate uploaded files.** Uploaded files should be checked for file size and type, and scanned for malware if necessary. Consider what would happen if someone uploaded a Word or PDF file with an embedded virus that was widely distributed.

Error Handling

- **Security-related errors should throw exceptions.** Use throw/catch for all security-related exceptions, such authorization failures.
- **Security-related errors should be logged.** See the Accountability section for more details.
- **Technical details should never be displayed to users.** Applications in production should not display verbose error messages that include stack traces, configuration data or other technical information.
- Display generic error messages
- No unhandled exceptions
- Suppress framework-generated errors.
- Log all authentication activities
- Log all privilege changes
- Log administrative activities
- Log access to sensitive data
- Do not log inappropriate data
- Store logs securely
- Operations on Non-public Data should be logged
- Authorization failures should be logged
- Log entries should include date, time, username, IP address and description

Encryption

- **Require TLS.** All applications that require authentication should only be accessible over TLS 1.2 or later with 128-bit or larger key size. The application should reject attempts to use it over non-TLS connections. Cookies must never be set or transmitted without TLS, prior to authentication and encryption.

- **Use platform-supplied encryption tools.** If an application requires encryption, use the ASP.Net encryption libraries. Do not attempt to write your own encryption routines or random-number generators.
- **Seek guidance about complex encryption needs.** If you are considering using database encryption, symmetric encryption for distributed files, or any other potentially complicated encryption system, please speak with the Office of Information Security.
- **Do not use insecure FTP**. Regular FTP does not use encryption. This means that all passwords and data are transmitted in clear text. Use a web-based file distribution system, FTPS, SFTP or FTP over SSH instead.
- Use SSL Everywhere
- Disable HTTP access for all SSL enabled resources
- Use the Strict-Transport-Security header
- Securely exchange encryption keys
- Setup secure key management processes
- Disable weak SSL ciphers on servers
- Use valid SSL certificates from a reputable CA
- Disable data caching using cache control headers and autocomplete
- Limit the use and storage of sensitive data.

Attachment C: BOE Parents' Bill of Rights for Data Privacy and Security

Both state and federal laws protect the confidentiality of information about your child that identifies him or her. Such information, which includes student-specific data, is known as "personally identifiable information." Under New York state's education law, if you are a parent of a child in the New York City public school district (the NYC DOE), you have the following rights regarding the privacy and security of your child's personally identifiable information and data.

(1) Your child's personally identifiable information cannot be sold or released for any commercial purposes.

(2) If your child is under age 18, you have the right to inspect and review the complete contents of your child's education records.

(3) Safeguards must be in place to protect your child's personally identifiable data when it is stored or transferred. These safeguards must meet industry standards and best practices. Examples of such safeguards include encryption, firewalls and password protection.

(4) You have the right to make complaints about possible breaches of student data and to have such complaints addressed. Complaints to the SED should be directed in writing to the Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany NY 12234, email to CPO@mail.nysed.gov. Complaints to the NYC DOE should be directed via email to data-security@schools.nyc.gov, or in writing to the Office of the Chief Information Officer, the Division of Instructional and Information Technology, New York City Department of Education, 335 Adams Street, Brooklyn NY 11201.

(5) You have additional rights as a parent, including additional privacy rights under federal law. They are found in the NYC DOE's Parents' Bill of Rights and Responsibilities, available here: https://www.schools.nyc.gov/school-life/policies-for-all/parents-bill-of-rights

(6) You can find a complete list of all of the types of student data that the New York State Education Department (SED) collects at this web-link:
http://www.p12.nysed.gov/irs/sirs/documentation/NYSEDstudentData.xlsx

You may also obtain a copy of this list by writing to the Office of Information & Reporting Services, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, NY 12234.

Attachment C: BOE Parents' Bill of Rights for Data Privacy and Security: Supplemental Information

Entity Name: HashCore DLT Inc. dba Rover Labs

New York Education Law §2-d requires the New York City Department of Education (NYC DOE) to supplement its Parents' Bill of Rights for Data Privacy and Security with additional information concerning agreements under which personally identifiable student information (Protected Information) is disclosed. In accordance with these provisions, it is necessary for you to provide the following. If an item is not applicable to your agreement, please explain why.

(1) The exclusive purposes for which Protected Information will be used, and how students and staff members will benefit from the Contractor's services:

Protected Information will be used by Rover Labs ("Rover") for the sole purpose of performing COVID-19 testing under its contractual agreement with New York City Health and Hospitals Corporation.

(2) How you will ensure that the subcontractors or other authorized persons or entities that you will share the student data or teacher or principal data with, if any, will abide by data protection and security requirements required by your written agreement with the NYC DOE:

Rover will not utilize any subcontractors for the testing, and will only report COVID-19 test results to the patients (or, if a minor, the parent or guardian), the ordering physician, and public health authorities including the Centers for Disease Control and Prevention, the NYS Department of Health, the NYC Department of Health, and NYC Health + Hospitals' NYC Test + Trace program as required or permitted by law.

(3) When the written agreement with the NYC DOE starts and ends and what happens to Protected Information upon expiration of the agreement:

This Agreement is effective Rover and will continue for so long as the Contractor will be providing the NYC DOE services with respect to COVID-19 testing. Protected Information will be permanently deleted at the end of the provision of services, except to the extent retention of test orders and requisitions, consents to testing, and test results are otherwise required by law, including but not limited to the federal Clinical Laboratory Improvement Amendments of 1988, as well as New York state laboratory laws and regulations. This Protected Information will be retained in the same secure manner as Rover retains information for the approximately 1,300 – 10,000 tests that it performs daily.

(4) If and how a parent, student, esligible student, teacher or principal may challenge the accuracy of the student data or teacher or principal data that is collected:

Pursuant to its contractual obligations, the Contractor will work with the NYC DOE in processing requests for copies of student Protected Information, and challenges to the accuracy of student data in the custody of the Contractor. Such requests should be directed to studentprivacy@schools.nyc.gov. However, if a parent of a student who was tested wishes to obtain a copy of their child's laboratory testing records, the request should be directed to schools.nyc.gov@rover-labs.com.

(5) Whether the Protected Information will be stored in the US or outside of the US (and if outside of the US, where), and the security protections taken to ensure such data will be protected (described in such a manner as to protect data security):

The Protected Information is stored in the US. Please see question #3 above.

(6) How the data will be encrypted (described in such a manner as to protect data security):

Rover employs industry standard encryption method and strength for data at rest and in transit.

Attachment D: Certificate of Records Disposal

CERTIFICATE OF RECORDS DISPOSAL

□ **The information described below was destroyed in the normal course of business pursuant to organizational retention schedule destruction policies and procedures, and/or written agreement.**

Description of Information Disposed Of/Destroyed:
□ Noted in Attachment

PERSON PERFORMING SANITIZATION

Name:	Title:	
Organization:	Location:	Phone:

MEDIA INFORMATION

Make/Vendor:	Model Number:
Serial Number(s)/Property Numbers:	
Media Type:	Source (i.e., user name/property #):
Data Classification:	Data Backed up? □ Yes □ No □ Unknown
Backup Location (if applicable):	

SANITIZATION DETAILS

Method Type:	□ Clear	□ Purge	□ Damage	□ Destruct	□ Other:
Method Used:	□ Degauss	□ Overwrite	□ Block Erase	□ Crypto Erase	□ Other:

Method Details:

Tool Used (include version):

Verification Method: □ Full □ Quick Sampling □ Other:

Post-Sanitization Classification:

Notes:

MEDIA DESTINATION

□ Internal Reuse □ External Reuse □ Recycling Facility □ Manufacturer □ Other (specify in Details)

Details:

SIGNATURE

□ I attest that the information provided on this Certification of Destruction and Sanitization is accurate to the best of my knowledge.

Signature: Date:

VALIDATION

Name:	Title:	
Organization:	Location:	Phone:
Signature:		Date: