PARENT BILL OF RIGHTS FOR STUDENT
DATA PRIVACY AND SECURITY
THIRD PARTY CONTRACTOR SUPPLEMENT

Incident IQ, LLC ("iiQ") has been engaged by the City School District of Albany to provide services. In this capacity, the company may collect, process, manage, store or analyze student and/or teacher/principal personally identifiable information (PII).

iiQ will provide the district with cloud software services for IT ticketing, asset management, etc.

iiQ will ensure that subcontractors or others that the company shares PII with will abide by data protection and security requirements of district policy, and state and federal law and regulations by contractually requiring such if/when subcontractors are utilized in the provision of the contracted-for Cloud Services. iiQ, by entering into an Agreement with the School District acknowledges it has reviewed the relevant District policies on safeguarding PII, including but not limited to, Policy 8635 and Regulation 8635.

PII will be stored in servers physically secured in the Microsoft Azure data centers, regions East US (Virginia), East US 2 (Virginia), and West US (California).

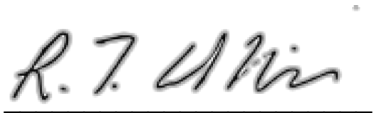
Parents may challenge the accuracy of PII held by iiQ by contacting R.T. Collins, Chief Operating Officer, 519 Memorial Drive SE, Ste B-12, Atlanta, GA 30312; phone: (470) 737-3505; email: rtcollins@incidentiq.com.

iiQ will take reasonable measures to ensure the confidentiality of PII by implementing the following:

- We will operate the Cloud Services and collect, process and store Protected Data in accordance with NIST data security standards and current industry best practices, and maintain all technologies, policies, procedures and practices necessary to secure and protect the confidentiality and integrity of Protected Data, and prevent unauthorized access, disclosure and use.
- Administrative procedures: Customer support representatives accordingly confirm caller identity against a District's list of administrator-users. Account creation and deletion is controlled by the District as user profiles are established through syncing with the client's identity management provider (e.g., Microsoft ADFS, Google SSO, local Active Directory, etc.). Accordingly, account creation/deletion is managed by the District through their ordinary identity management policies and procedures. Also, permissions modification of any given user may be managed by the clients' administrator-level users through tools in their admin console. If assistance were required in this process admin-users would authenticate with customer support representatives as described above.
- Encryption while PII is in motion and at rest: Data in transit are SSL protected, as well as Protected Data are always encrypted. Any data designated as Protected Data which include passwords, is encrypted within the database using combinations of one-way and two-way encryption algorithms (such as SHA256) with Salt strings.

- Firewalls: All information is stored within databases hosted and secured within the Microsoft Azure Cloud. The Azure cloud is secured with actively monitored network firewalls, intrusion detection systems, application firewalls, and IP-route protection. Additionally, any information designated as Protected Data is encrypted within the database.
- Other: See Exhibit A, attached hereto

The contractor's agreement with the district begins on 5/4/2021 and ends on 8/3/2022. Once the contractor has completed its service to the district, records containing student PII will be: destroyed or returned) by sixty (60) days from the date of contract termination via a nonrecoverable deletion process in accordance with Department of Defense standard 5220.22-M.



8 June 2021

Authorized Representative
R.T. Collins, Chief Operating Officer
Incident IQ, LLC

Date

EXHIBIT A
DATA PRIVACY AND SECURITY PLAN

CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN IS ATTACHED HERETO AND INCORPORATED HEREIN.

Incident IQ, LLC ("Incident IQ, We, Us, or Our"), as a covered third-party contractor Education Law 2-d shall undertake all of the following data privacy, security, and protection measures, in addition to the requirements already contained in the Incident IQ Cloud Services Master Subscription Agreement:

1. Data Collection & Use:
    a. Incident IQ shall only collect only collect, process and store such Protected Data to which we have a legitimate educational interest and as is necessary to provide the cloud services.
    b. Under no circumstances will Incident IQ use Protected Data to market or advertise to students or their family members or legal guardians, or otherwise use Protected Data to inform, influence or enable marketing, advertising or other commercial efforts by a third party directed at students, their family members, or legal guardians.
    c. We shall not change how Protected Data are collected maintained, used or disclosed under the terms of the Agreement, without advance notice to and prior written consent from District.
    d. We will never sell Protected Data that we acquire through District use of the Cloud Services, except as part of a corporate purchase, merger or other type of acquisition. In such a case, any successor entity shall be contractually obligated to comply with the terms of this Agreement related to the treatment of Protected Data, as well as all other applicable legal requirements governing the use, disclosure, and security of the previously acquired Protected Data.

2. Data Portability: Incident IQ shall ensure the data portability of all District data.
    a. Upon notice of a request from District for a copy of certain Protected Data in Our possession (e.g., to support the District's response to a properly constituted request for Protected Data from a parent, guardian or student), we will ensure that: (i) A complete and readable digital copy of the requested Protected Data in Incident IQ's possession is delivered to District within 30 days of our receipt of District's request; (ii) Upon delivery of the copy, District must provide notice to Incident IQ of District's receipt and acceptance of any such requested Protected Data;
    b. Upon notice of a request from District that certain Protected Data be deleted, We will permanently destroy (i.e., undertake a non-recoverable deletion process in accordance with Department of Defense standard 5220.22-M) all copies of the Protected Data identified for deletion by District held by Us or any of Our agents, subcontractors or affiliates. Within 30 days of District notice, we will deliver a written confirmation to District certifying that the permanent destruction of the requested Protected Data has been accomplished. Upon delivery of such written confirmation of deletion, District must provide notice to Us of District receipt and understanding of said notice confirming deletion made at District request.
    c. We shall destroy all Protected Data residing in District's instance of the Cloud Services, using the methods described in paragraph 2(b) above, following expiration of a 60-day period after termination of this Agreement, unless District requests that We return such information to District instead.

3. Data Security:

a. We will operate the Cloud Services and collect, process and store Protected Data in accordance with NIST data security standards and current industry best practices, and maintain all technologies, policies, procedures and practices necessary to secure and protect the confidentiality and integrity of Protected Data, and prevent unauthorized access, disclosure and use.
b. All information is stored within databases hosted and secured within the Microsoft Azure Cloud. The Azure cloud is secured with actively monitored network firewalls, intrusion detection systems, application firewalls, and IP-route protection. Additionally, any information designated as Protected Data is encrypted within the database.
c. No data shall be stored outside the United States; all data are stored in the Microsoft Azure data center, region East US (Virginia), East US 2 (Virginia), and/or West US (California).
d. Any data designated as Protected Data which include passwords, is encrypted within the database using combinations of one-way and two-way encryption algorithms (such as SHA256) with Salt strings.
e. Information is multi-tenanted and stored within the same cloud systems; however, all information is partitioned by a School District ID (i.e., SiteId) and the Data Access Layers forces all data to be filtered by a specific School District.
f. Physical servers are physically secured in the Microsoft Azure data centers, regions East US (Virginia), East US 2 (Virginia), and West US (California).
g. Data in transit are SSL protected, as well as Protected Data are always encrypted.
h. Only Incident IQ Senior Technical Team members have direct access to product data. All personnel with access to Incident IQ systems and data are vetted via backgrounds checks and receive annual and update training on all relevant policies and procedures.
i. No software functions are subcontracted to other vendors apart from the hosting/storage services provided by Microsoft, as described above.
j. Customer support representatives accordingly confirm caller identity against a District's list of administrator-users. Account creation and deletion is controlled by the District as user profiles are established through syncing with the client's identity management provider (e.g., Microsoft ADFS, Google SSO, local Active Directory, etc.). Accordingly, account creation/deletion is managed by the District through their ordinary identity management policies and procedures. Also, permissions modification of any given user may be managed by the clients' administrator-level users through tools in their admin console. If assistance were required in this process admin-users would authenticate with customer support representatives as described above.

4. Network Operations Center Management and Security:
    a. Incident IQ shall perform regular penetration testing, vulnerability management and intrusion prevention testing.
    b. All network devices shall be located in secure facilities under controlled circumstances (*i.e.,* ID cards and entry logs) at the Microsoft Azure data centers, regions East US (Virginia), East US 2 (Virginia), and West (California).
    c. Backups shall be performed daily (to other US-based Azure Data Centers), as well as backups made to separate secure, off-site facility.
    d. Backups shall be encrypted and stored securely with access limited to administrators with restoration encryption keys.
    e. All software vulnerabilities shall be patched routinely or automatically in accordance with the following parameters: all critical and High vulnerabilities shall be patched automatically. Medium vulnerabilities shall be patched monthly during planned maintenance windows. Low vulnerabilities shall be evaluated and if deemed necessary, shall be patched during the planned monthly maintenance window.