



Kenton County School District | *It's about ALL kids.*

Issue Paper

DATE:

6/17/2024

AGENDA ITEM (ACTION ITEM):

Consider/Approve the purchase of Incident IQ for Technology Help Desk software and corresponding Asset Management system.

APPLICABLE BOARD POLICY:

01.1 Legal Status of the Board

HISTORY/BACKGROUND:

KCSD Technology has utilized various forms of free help desk software over the last few years. We have out grown those systems and are currently processing nearly 8200+ work orders each year. There is a need for enhanced functionality, reporting, and routing that a paid system can offer. KCSD Technology have reviewed multiple systems and identified Incident IQ as the product that will service our current and future needs. Additionally, this product directly integrates with multiple other services the district already utilizes for a seamless end user and operator experience that directly results in efficient and timely responses. Secondly, the district currently leverages Follett School Solutions for asset management. With this proposal and support of the Finance Department, it is also recommended that we move the asset management to Incident IQ to create a complete experience for the management of the district assets. Training will be provided to all end users and operators. This system would be utilized by all schools and enhance the efficiency of the Technology Department in their response to work orders.

FISCAL/BUDGETARY IMPACT:

\$55,385.12 (Technology and Finance Funds)

RECOMMENDATION:


Approval of the purchase of Incident IQ for Technology Help Desk software and corresponding Asset Management system.

CONTACT PERSON:

Matthew Winkler, Director of Technology


Principal/Administrator


District Administrator


Superintendent

Use this form to submit your request to the Superintendent for items to be added to the Board Meeting Agenda.

Principal –complete, print, sign and send to your Director. Director –if approved, sign and put in the Superintendent’s mailbox.



Quote Name Kenton - iiQ Ticketing & Assets
Company Address 750 Glenwood Ave SE Suite 320
 Atlanta, GA 30316
 US

Created Date	6/17/2024
Expiration Date	7/31/2024
Quote Number	41909

Contract Start Date 7/1/2024
Contract End Date 6/30/2025

Contact Name	Matthew Winkler
Phone	(859)344-8888

Bill To Name Kenton County
Bill To 1055 Eaton Dr
Fort Wright, KY 41017
United States

Ship To Name **Kenton County**
Ship To **1055 Eaton Dr**
 Fort Wright, KY 41017
 United States

Product Code	Product	Product Description	Sales Price	Quantity
IIQ-1000	iiQ Platform with Ticketing	Incident IQ Platform with iiQ Ticketing core product, Subscription	\$29,668.82	1.00
IIQ-6200	iiQ Assets	Incident IQ Assets product (add-on), Subscription	\$20,768.17	1.00
IIQ-9000	iiQ Launchpad On-boarding Services	Implementation of Incident IQ Cloud Services, one-time fee	\$4,948.13	1.00

Total Price	\$55,385.12
--------------------	--------------------

Notes

Pricing Pursuant to TIPS contract #220105, district is receiving a 2.5% discount.

Kenton will have access to begin implementation, and receive a no-charge period from purchase order delivery date to the contract start date above.

All Incident IQ products and services are purchased and delivered pursuant to the Incident IQ Cloud Services Master Subscription Agreement, as found at <https://www.incidentiq.com/legal/master-services-agreement>, along with any applicable Supplements (available at <https://www.incidentiq.com/legal>). All of the aforementioned are incorporated into this ordering document by reference to the maximum extent permitted by local, state, and federal laws and regulations. For any legal questions, please contact us at legal@incidentiq.com.



Kenton County School District | It's about ALL kids

THE KENTON COUNTY BOARD OF EDUCATION

1055 EATON DRIVE, FORT WRIGHT, KENTUCKY 41017

TELEPHONE: (859) 344-8888 / FAX: (859) 344-1531

WEBSITE: www.kenton.kyschools.us

Dr. Henry Webb, Superintendent of Schools

VENDOR ASSURANCES REGARDING PROTECTION OF PERSONAL AND CONFIDENTIAL INFORMATION

Data Security and Breach Protocols

Vendors that receive Personal Information from Kenton County Board of Education (herein referred to as "KCBOE") as defined by and in accordance with Kentucky's Personal Information Security and Breach Investigation Procedures and Practices Act, KRS 61.931, et seq., (the "Act"), shall secure and protect the Personal Information by, without limitation, complying with all requirements applicable to non-affiliated third parties set forth in the Act.

"Personal Information" is defined in accordance with KRS 61.931(6) as "an individual's first name or first initial and last name; personal mark; or unique biometric or genetic print or image, in combination with one (1) or more of the following data elements:

- a) An account number, credit card number, or debit card number that, in combination with any required security code, access code or password, would permit access to an account;
- b) A Social Security number;
- c) A taxpayer identification number that incorporates a Social Security number;
- d) A driver's license number, state identification card number or other individual identification number issued by any agency as defined under the Act;
- e) A passport number or other identification number issued by the United States government; or
- f) Individually Identifiable Information as defined in 45 C.F.R. sec. 160.013 (of the Health Insurance Portability and Accountability Act), except for education records covered by the Family Education Rights and Privacy Act, as amended 20 U.S.C. sec 1232g."

As provided in KRS 61.931(5), a "non-affiliated third party" includes any person or entity that has a contract or agreement with the KCBOE and receives (accesses, collects or maintains) personal information from the KCBOE pursuant to the contract or agreement.

The vendor hereby agrees to cooperate with the KCBOE in complying with the response, mitigation, correction, investigation, and notification requirements of the Act.

The vendor shall notify as soon as possible, but not to exceed seventy-two (72) hours, KCBOE, the Commissioner of the Kentucky State Police, the Kentucky Auditor of Public Accounts, the Commonwealth (Kentucky) Office of Technology, and the Commissioner of the Kentucky Department of Education of a determination of or knowledge of a breach, unless the exception set forth in KRS 61.932(2)(b)(2) applies and the vendor abides by the requirements set forth in that exception. Notification shall be in writing on a form developed by the Commonwealth (Kentucky) Office of Technology.

The vendor hereby agrees to report to the KCBOE, immediately and within twenty-four (24) hours, any known reasonably believed instances of missing data, data that has been inappropriately shared, or data taken off site.

The vendor hereby agrees that the KCBOE may withhold payment(s) owed to the vendor for any violation of the Act's notification requirements.

The vendor hereby agrees to undertake a prompt and reasonable investigation of any security breach as defined under the Act in accordance with KRS 61.933.

Upon conclusion of an investigation of a security breach as defined under the Act as required by KRS 61.933, the vendor hereby agrees to an apportionment of the costs of the notification, investigation, and mitigation of the security breach.

In accordance with KRS 61.932(2)(a), the vendor shall implement, maintain, and update security and breach investigation procedures that are appropriate to the nature of the information disclosed, that are at least as stringent as the security and breach investigation procedures and practices established by the Commonwealth (Kentucky) Office of Technology and that are reasonably designed to protect the Personal Information from unauthorized access, use, modification, disclosure, manipulation, or destruction.

Student Data Security

Pursuant to KRS 365.734, if the vendor is a cloud computing service provider (which is defined pursuant to KRS 365.734(1)(b) as any person or entity other than an educational institution that operates cloud computing services) or, through service to the KCBOE, becomes the equivalent of a cloud computing service provider, the vendor further hereby agrees that:

- The vendor shall not process student data as defined pursuant to KRS 365.734 for any purpose other than providing, improving, developing, or maintaining the integrity of its cloud computing services, unless the vendor receives express permission from the student's parent. The vendor shall work with the KCBOE to determine the best method of collecting parental permission.
- With a written agreement for educational research, the vendor may assist the KCBOE to conduct educational research as permitted by the Family Education Rights and Privacy Act of 1974, as amended, 20 U.S.C. sec. 1232g.
- Pursuant to KRS 365.734, the vendor shall not in any case process student data to advertise or facilitate advertising or to create or correct an individual or household profile for any advertisement purposes.
- Pursuant to KRS 365.734, the vendor shall not sell, disclose, or otherwise process student data for any commercial purpose.
- Pursuant to KRS 365.734, the vendor shall certify in writing to the agency that it will comply with KRS 365.734(2).

Family Educational Rights and Privacy Act, National School Lunch Act and Child Nutrition Act

If during the course of this agreement, the KCBOE discloses to the vendor any data protected by the Family Educational Rights and Privacy Act of 1974 (FERPA), as amended (20 U.S.C. sec. 1232g, *et seq.*), and its regulations, and data protected by the Richard B. Russell National School Lunch Act (NSLA) (42 U.S.C. sec. 1751 *et seq.*), and the Child Nutrition Act of 1966 (CNA) (42 U.S.C. sec. 1771 *et seq.*), the vendor agrees that it is bound by and will comply with the confidentiality, security and redisclosure requirements and restrictions stated in FERPA, NSLA and CNA.

The vendor hereby agrees to report to the KCBOE, immediately and within twenty-four (24) hours, any known reasonably believed instances of missing data, data that has been inappropriately shared, or data taken off site.

The vendor agrees that FERPA-protected information is confidential information. FERPA-protected information includes, but is not limited to the student's name, the name of the student's parent or other family members, the address of the student or student's family, a personal identifier, such as the student's social security number, student number, or biometric record, other indirect identifiers, such as the student's date of birth, place of birth, and mother's maiden name, and other information that, alone or in combination, is linked or linkable to a specific

student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty.

The vendor understands and acknowledges that any unauthorized disclosure of confidential information is illegal as provided in FERPA and in the implementing federal regulations found in 34 CFR, Part 99. The penalty for unlawful disclosure is a fine of not more than \$250,000 (under 18 U.S.C. sec. 3571) or imprisonment for not more than five years (under 18 U.S.C. sec. 3559), or both.

The vendor understands and acknowledges that children's free and reduced price meal and free milk eligibility information or information from the family's application for eligibility, obtained under provisions of the NSLA or the CNA is confidential information and that any unauthorized disclosure of confidential free and reduced price lunch information or information from an application for this benefit is illegal. The penalty for unlawful disclosure is a fine of not more than \$1,000.00 (under 7 C.F.R. 245.6) or imprisonment for up to one year (under 7 C.F.R. 245.6), or both.

In the event there is a conflict between this agreement and any other agreement between KCBOE and Vendor, the terms of this agreement shall apply.

Incident IQ, LLC
Vendor Name

750 Glenwood Ave SE Suite 320, Atlanta, GA 30316
Vendor Address

(866) 488-3102; 630-651-1522
Vendor Telephone

accounting@incidentiq.com ; legal@incidentiq.com
Vendor Email Address


Signature by Vendor's Authorized Representative

Donato Latrofa
Print Name

6/18/2024
Date

Request for Taxpayer Identification Number and Certification

Give Form to the
requester. Do not
send to the IRS.

► Go to www.irs.gov/FormW9 for instructions and the latest information.

Print or type.
See Specific Instructions on page 3.

1 Name (as shown on your income tax return). Name is required on this line; do not leave this line blank.

Incident IQ, LLC

2 Business name/disregarded entity name, if different from above

3 Check appropriate box for federal tax classification of the person whose name is entered on line 1. Check only **one** of the following seven boxes.

☐ Individual/sole proprietor or single-member LLC

☐ C Corporation

☐ S Corporation

☐ Partnership

☐ Trust/estate

☒ Limited liability company. Enter the tax classification (C=C corporation, S=S corporation, P=Partnership) ► **P**

Note: Check the appropriate box in the line above for the tax classification of the single-member owner. Do not check LLC if the LLC is classified as a single-member LLC that is disregarded from the owner unless the owner of the LLC is another LLC that is **not** disregarded from the owner for U.S. federal tax purposes. Otherwise, a single-member LLC that is disregarded from the owner should check the appropriate box for the tax classification of its owner.

☐ Other (see instructions) ►

4 Exemptions (codes apply only to certain entities, not individuals; see instructions on page 3):

Exempt payee code (if any) _____

Exemption from FATCA reporting code (if any) _____

(Applies to accounts maintained outside the U.S.)

5 Address (number, street, and apt. or suite no.) See instructions.

750 Glenwood Ave SE, Suite 320

6 City, state, and ZIP code

Atlanta GA 30316

Requester's name and address (optional)

7 List account number(s) here (optional)

Part I Taxpayer Identification Number (TIN)

Enter your TIN in the appropriate box. The TIN provided must match the name given on line 1 to avoid backup withholding. For individuals, this is generally your social security number (SSN). However, for a resident alien, sole proprietor, or disregarded entity, see the instructions for Part I, later. For other entities, it is your employer identification number (EIN). If you do not have a number, see *How to get a TIN*, later.

Note: If the account is in more than one name, see the instructions for line 1. Also see *What Name and Number To Give the Requester* for guidelines on whose number to enter.

Social security number

____ - ____ - _____

or

Employer identification number

8 1 - 3 6 7 6 8 7 1

Part II Certification

Under penalties of perjury, I certify that:

- The number shown on this form is my correct taxpayer identification number (or I am waiting for a number to be issued to me); and
- I am not subject to backup withholding because: (a) I am exempt from backup withholding, or (b) I have not been notified by the Internal Revenue Service (IRS) that I am subject to backup withholding as a result of a failure to report all interest or dividends, or (c) the IRS has notified me that I am no longer subject to backup withholding; and
- I am a U.S. citizen or other U.S. person (defined below); and
- The FATCA code(s) entered on this form (if any) indicating that I am exempt from FATCA reporting is correct.

Certification instructions. You must cross out item 2 above if you have been notified by the IRS that you are currently subject to backup withholding because you have failed to report all interest and dividends on your tax return. For real estate transactions, item 2 does not apply. For mortgage interest paid, acquisition or abandonment of secured property, cancellation of debt, contributions to an individual retirement arrangement (IRA), and generally, payments other than interest and dividends, you are not required to sign the certification, but you must provide your correct TIN. See the instructions for Part II, later.

Sign
Here

Signature of
U.S. person ►

Donato / 12/14

Date ► **13 January 2024**

General Instructions

Section references are to the Internal Revenue Code unless otherwise noted.

Future developments. For the latest information about developments related to Form W-9 and its instructions, such as legislation enacted after they were published, go to www.irs.gov/FormW9.

Purpose of Form

An individual or entity (Form W-9 requester) who is required to file an information return with the IRS must obtain your correct taxpayer identification number (TIN) which may be your social security number (SSN), individual taxpayer identification number (ITIN), adoption taxpayer identification number (ATIN), or employer identification number (EIN), to report on an information return the amount paid to you, or other amount reportable on an information return. Examples of information returns include, but are not limited to, the following.

- Form 1099-INT (interest earned or paid)

- Form 1099-DIV (dividends, including those from stocks or mutual funds)
- Form 1099-MISC (various types of income, prizes, awards, or gross proceeds)
- Form 1099-B (stock or mutual fund sales and certain other transactions by brokers)
- Form 1099-S (proceeds from real estate transactions)
- Form 1099-K (merchant card and third party network transactions)
- Form 1098 (home mortgage interest), 1098-E (student loan interest), 1098-T (tuition)
- Form 1099-C (canceled debt)
- Form 1099-A (acquisition or abandonment of secured property)

Use Form W-9 only if you are a U.S. person (including a resident alien), to provide your correct TIN.

If you do not return Form W-9 to the requester with a TIN, you might be subject to backup withholding. See What is backup withholding, later.

INCIDENT IQ CLOUD SERVICES MASTER SUBSCRIPTION AGREEMENT (MSA)

Revised January 1, 2023,

Effective January 8, 2023

THIS AGREEMENT GOVERNS YOUR ACQUISITION AND USE OF OUR CLOUD SERVICES.

THE APPLICABLE PROVISIONS OF THIS AGREEMENT ALSO GOVERN ANY PILOT TRIAL. THE TERMS OF THIS AGREEMENT EXPRESSLY SUPERSEDE ALL PRIOR TERMS OF ALL PRIOR AGREEMENTS. **THIS AGREEMENT APPLIES TO ALL AGREEMENTS ENTERED INTO ON AND AFTER JANUARY 8, 2023;** AGREEMENTS PREDATING THIS AGREEMENT SHALL BE GOVERNED BY THE TERMS APPLICABLE AT THE DATE OF EXECUTION.

YOU ACCEPT THE TERMS OF THIS MSA BY EXECUTING AN "ORDER FORM" AND/OR PILOT SERVICE AGREEMENT THAT REFERENCES THIS AGREEMENT. IF YOU ARE ENTERING INTO THIS AGREEMENT ON BEHALF OF A SEPARATE LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS AND CONDITIONS, IN WHICH CASE THE TERMS "YOU" OR "YOUR" SHALL REFER TO SUCH ENTITY. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT AGREE WITH THESE TERMS AND CONDITIONS, YOU MUST NOT ACCEPT THIS AGREEMENT AND MAY NOT USE THE CLOUD SERVICES.

1 DEFINITIONS

- 1.1 "Acceptable Use Policy" or "AUP" is defined in [Section 2](#).
- 1.2 "Affiliate" means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity.
- 1.3 "Agreement" means this Master Subscription Agreement.
- 1.4 "Cloud Services" means products using Our proprietary cloud service, ("Incident IQ Platform" or "iiQ Platform" or "Platform") and any related offerings, as identified in the relevant Order and as modified from time to time. The Cloud Service includes Our Software and Documentation but not Professional Services deliverables or Third-Party Content.
- 1.5 "Content" means information obtained by Incident IQ from publicly available sources or third-party content providers and made available to You through the Cloud Services or pursuant to an Order Form.

- 1.6 “Confidential Information” means information disclosed by or on behalf of one party (as discloser) to the other party (as recipient) under this Agreement, in any form, which (a) the discloser identifies to recipient as “confidential” or “proprietary” or (b) should be reasonably understood as confidential or proprietary due to its nature and the circumstances of its disclosure. Our Confidential Information includes technical or performance information about the Cloud Service, and Customer’s Confidential Information includes Customer Data.
- 1.7 “Customer” means the party purchasing Cloud Services from Us.
- 1.8 “Customer Data” means any data, content or materials that Customer (including its Users and any other interested stakeholders) uploads into, enters into, or submits to its Cloud Service accounts, including from Third-Party Platforms. For clarification, Customer Data excludes Usage Data (defined [below](#)).
- 1.9 “Customer Materials” means materials and resources that Customer makes available to Provider in connection with Professional Services.
- 1.10 “Documentation” means Our standard usage documentation for the Cloud Services.
- 1.11 “Effective Date” means the first day that Customer has access to the Cloud Services purchased with an Order Form.
- 1.12 “Feedback” means any information provided by You to Incident IQ regarding an existing or potential future product, service, or other performance provided by or sought from Incident IQ.
- 1.13 “Force Majeure” means an unforeseen event beyond a party’s reasonable control, such as a strike, blockade, war, pandemic, act of terrorism, riot, third-party Internet or utility failure, refusal of government license or natural disaster, where the affected party takes reasonable and customary measures to avoid or mitigate such event’s effects.
- 1.14 “Laws” means all laws, regulations, rules, court orders or other binding requirements of a governmental authority that apply to a party.
- 1.15 “Order Form” means an ordering document or online order specifying the Cloud Services and related services to be provided by Us under the terms of this Master Subscription Agreement (MSA), including any addenda and supplements thereto. Typically includes a purchase order submitted by You in response to a price quotation (“quote”) provided by Us or a third party authorized by Us to resell the Cloud Services. The purchase order and the quote together constitute an “Order Form” for the

purposes of any relevant Agreement.

- 1.16 “Personal Data” means Customer Data relating to an identified or identifiable natural person.
- 1.17 “Protected Student Information” means “Student Personally Identifiable Information” or “Student Education Records,” within the meaning of the Family Educational Rights and Privacy Act (FERPA) of 1974 and its related provisions under the Code of Federal Regulations, as well as any applicable related state or local laws or regulations
- 1.18 “Professional Services” means any training, data migration or other professional services that We furnish to You related to the Cloud Services.
- 1.19 “Renewal” is the process by which the Services Period of certain Cloud Services under an Order Form is extended for an additional Services Period beyond the initial term, unless such Cloud Services are otherwise terminated in accordance with the terms of the Order Form or this Agreement. Your Order Form defines which Cloud Services are eligible for Renewal as well as any terms applicable to any such renewal.
- 1.20 “Services Period” refers to the period of time for which You ordered the Cloud Services as specified in any Order Form.
- 1.21 “Statement of Work” means a statement of work for Professional Services that is executed by the parties and references this Agreement.
- 1.22 “Support” means support provided by Us to Customers for the onboarding and use of the Cloud Services, as governed by the [Support Policy](#).
- 1.23 “Support Policy” is defined in [Support Policy](#).
- 1.24 “Suspension Event” means (a) Customer’s account is 30 days or more overdue, (b) Customer is in breach of AUP, and/or (c) Customer’s use of the Cloud Service risks material harm to the Cloud Service or others.
- 1.25 “Third-Party Claim” means a claim, action, allegation, or other dispute described in [Defense & Indemnification](#) brought by a person, entity, or other party that is: (a) not a contracting party to this Agreement or an Order governed by this Agreement; or (b) is an Affiliate of a contracting party to this Agreement (except in the case of a Customer Affiliate that enters into a contract or Order directly with Us and such Order is governed by this Agreement).

- 1.26 “Third-Party Content” means all text, files, images, graphics, charts, tables, illustrations, information, applications, products, services, data, audio, video, photographs and other content and material, in any format, that are obtained or derived from third-party sources outside of Incident IQ and made available to You through, within, or in conjunction with Your use of, the Cloud Service.
- 1.27 “Usage Data” means Our technical logs, data and learnings about Your use of the Cloud Service, including, but not limited to, the number of reports run, the frequency of User log-ins, location of User log-ins, and User behavioral data, such as the types of searches run and features heavily used).
- 1.28 “User” means those employees, contractors, students, parents, staff, and/or end users, as applicable, authorized by You to use the Cloud Services in accordance with this Agreement and/or Your Order Form.
- 1.29 “We,” “Us” or “Our” means Incident IQ, LLC and its affiliates.
- 1.30 “You” or “Your” means the legal entity for which you are accepting this Agreement.

2 ACCEPTABLE USE POLICY (AUP):

2.1 You will be responsible for:

- 2.1.1 Users’ compliance with this Agreement and applicable Order Forms,
- 2.1.2 the accuracy, quality and legality of Your Data and the means by which You acquired Your Data;
- 2.1.3 using commercially reasonable efforts to prevent unauthorized access to or use of the Cloud Services and Content,
- 2.1.4 notifying Us promptly of any such unauthorized access or use;
- 2.1.5 using the Cloud Services and Content only in accordance with this Agreement, Order Forms, and applicable laws and government regulations, including, but not limited to, Children’s Online Privacy Protection (COPPA);
- 2.1.6 complying with terms of service of any Third-Party Content with which You use the Cloud Services.

2.2 You will not:

- 2.2.1 make the Cloud Services or Content available to, or use the Cloud Services or Content for the benefit of, anyone other than You or

authorized Users;

- 2.2.2 sell, resell, license, sublicense, distribute, make available, rent or lease the Cloud Services or Content;
 - 2.2.3 use the Cloud Services to store or transmit infringing, libelous, or otherwise unlawful or tortious material, or to store or transmit material in violation of third-party privacy rights;
 - 2.2.4 interfere with or disrupt the integrity or performance of the Cloud Services or third-party data contained therein;
 - 2.2.5 attempt to gain unauthorized access to the Cloud Services or Content or its related systems or networks;
 - 2.2.6 permit direct or indirect access to or use of the Cloud Services or Content in a way that circumvents a contractual usage limit, or use any of the Cloud Services to access or use any of Our intellectual property except as permitted under this Agreement or an Order Form;
 - 2.2.7 copy, reverse engineer, or attempt to reverse engineer the Cloud Services or any part, feature, function or user interface thereof;
 - 2.2.8 assist or advise any competitor in their attempts to engineer, reverse engineer, or otherwise copy the Cloud Services or any part, feature, function, or user interface thereof;
 - 2.2.9 copy Content except as permitted by Us in a written agreement;
 - 2.2.10 access the Cloud Services or Content in order to build a competitive product or service or to benchmark with a Non-Incident IQ product or service;
 - 2.2.11 otherwise misuse the Platform in any way contrary with the letter and intent of this Agreement or inconsistent with governing law and/or regulations.
 - 2.2.12 permit users under the age of 13 to use Incident IQ without ensuring all requirements and regulations under COPPA and related state/local regulations are strictly adhered to.
- 2.3 Any use of the Cloud Services in breach of this Agreement or applicable Order Form by You or Users, that in Our judgment threatens the security, integrity or availability of Our services, may result in immediate suspension of the Cloud Services; however, We will use commercially reasonable efforts under the circumstances to provide You with notice and an opportunity to remedy such violation or threat prior to such suspension.

- 2.4 You agree to accept all patches, bug fixes, updates, maintenance and service packs (collectively, "Patches") necessary for the proper function and security of the Cloud Services. Except for emergency or security-related maintenance activities, We will notify You of the scheduling of application of Patches, where possible.

3 INCIDENT IQ RIGHTS AND RESPONSIBILITIES

3.1 We will:

- 3.1.1 make all commercially reasonable efforts to provide the Cloud Services and Content available to You pursuant to this Agreement and the applicable Order Form;
- 3.1.2 provide applicable support for the Cloud Services as outlined in our [Support Policy](#) at no additional charge following completion of onboarding;
- 3.1.3 use commercially reasonable efforts to make the online Cloud Services available 24 hours a day, 7 days a week, except for:
 - 3.1.3.1 planned downtime (of which We shall give reasonable advance electronic notice), and**
 - 3.1.3.2 any unavailability caused by force majeure.**

3.2 We may:

- 3.2.1 Monitor, observe, compile, store, and/or analyze statistical and other information related to the performance, operation, and use of the Cloud Services;
- 3.2.2 Utilize Usage Data for security and operations management, to create statistical analyses, and for research and development purposes (clauses 3.2.1 and 3.2.2 are collectively referred to as "Service Analyses").
- 3.2.3 We may make Service Analyses publicly available; however, Service Analyses will not incorporate Your Data in a form that could serve to identify You or any individual. We retain all intellectual property rights in Service Analyses.

4 Intellectual Property

- 4.1 Neither party grants the other any rights or licenses not expressly set out in this Agreement. Except for Our express rights in this Agreement, as between the parties, Customer retains all intellectual property and other rights in Customer Data and Customer Materials provided to Us.
- 4.2 Except for Customer's express rights in this Agreement, as between the parties, We retain all intellectual property and other rights in the Cloud

Services, deliverables and related technology (including, but not limited to, all underlying software, source code, design, modules, organization, format, algorithm, and other technology), and all modifications or enhancements thereto and derivatives thereof.

- 4.3 We may use any Feedback from You or Your Users regarding improvement or operation of the Cloud Services, Support or Professional Services without restriction or obligation.
- 4.4 Feedback is provided "AS IS" and We will not publicly identify You as the source of feedback without Your permission.
- 4.5 Unless mutually agreed upon in a separate, fully-executed agreement, We have not agreed to and do not agree to treat as confidential any Feedback You provide to Us, and nothing in this Agreement or in the parties' dealings arising out of or related to this Agreement will restrict Our right to use, profit from, disclose, publish, keep secret, or otherwise exploit Feedback, without compensating or crediting You. Feedback will not be considered Customer's Confidential Information, intellectual property, or its trade secret. Once received by Us, such Feedback becomes Our Confidential Information, Intellectual Property, and/or trade secret.
- 4.6 You grant to Us a worldwide, perpetual, irrevocable, royalty-free license to use and incorporate into Our services any feedback suggestion, enhancement request, recommendation, correction or other feedback provided by You or Users relating to the operation of Our services.

5 SAFEGUARDS FOR YOUR DATA.

- 5.1 Subject to this Agreement, We will access and use Your Data solely to provide and maintain the Cloud Services, Support, and Professional Services under this Agreement. Such use includes sharing Your Data as You direct through the Cloud Services, but We will not otherwise disclose Customer Data to third-parties except as permitted in this Agreement, or otherwise required by law.
- 5.2 We will implement and maintain reasonable Security Measures that:
 - 5.2.1 Are consistent with all federal, state, and local law and regulations;
 - 5.2.2 Will use appropriate and reasonable technical and organizational measures designed to prevent unauthorized access, use, alteration or disclosure of Customer Data.
 - 5.2.3 Will be audited by an external auditor, at Our expense and no less

frequently than annually, to verify the adequacy of Our control measures according to SOC 2 standards and/or such other similar standards that are substantially equivalent to such control standards. Such audit will result in the generation of an audit report;

5.2.3.1 Such audit reports will be deemed Our Confidential Information, and

5.2.3.2 Such audit reports may be made available to You upon your request to legal@incidentiq.com and execution of a separate non-disclosure agreement provided by us. This provision does not constitute an entitlement by You to any such audit report.

5.2.3.3 Any release of such audit reports are at our sole discretion. We may provide any reason or no reason at all for deciding to disclose or not disclose an audit report.

5.3 For any of Your Data residing in the Cloud Services environment and identified by You or Your Users or the law as “Protected Student Information,” We will undertake the following measures with respect to such data:

5.3.1 Only collect, process and store such Protected Student Information as is necessary to provide the cloud services under this Agreement;

5.3.2 Under no circumstances will We use such information to market or advertise to students or their family members or legal guardians, or otherwise use such information to inform, influence or enable marketing, advertising or other commercial efforts by a third party directed at students, their family members, or legal guardians;

5.3.3 Shall not change how Protected Student Information is collected, maintained, used or disclosed under the terms of the Agreement, without advance notice to and prior written consent from You.

5.4 Upon notice of a request for a copy of certain Protected Student Information in Our possession from You or a Person authorized under federal, state, and/or local law and regulations, we will ensure that:

5.4.1 A complete and readable digital copy of the requested Protected Student Information in Our possession is delivered to You within 30 days (or the maximum time permitted under law, whichever is greater) of our receipt of Your request;

5.4.2 Upon delivery of the copy to a Person authorized under federal, state, and/or local law and regulations, we will notify You of such disclosure if permitted by law. Such notification will be within the timeframe outlined in 5.4.1 above.

5.4.3 Such notice under 5.4 must be submitted to legal@incidentiq.com to constitute “notice” under section 5.4.

5.5 Upon notice of a request from You that certain Protected Student Information be deleted, we will:

5.5.1 permanently destroy (i.e., undertake a nonrecoverable deletion process in accordance with Department of Defense standard 5220.22-M) all copies of the Protected Student Information identified for deletion by You held by Us or any of Our agents, subcontractors or affiliates; and

5.5.2 Within 30 days of Your notice, we will deliver a written confirmation to You certifying that the permanent destruction of the requested Protected Student Information has been accomplished. Upon delivery of such written confirmation of deletion, you must provide notice to Us of Your receipt and understanding of said notice confirming deletion made at Your request.

5.5.3 Such notice under 5.5 must be submitted to legal@incidentiq.com to constitute “notice” under section 5.5

5.6 Regardless of whether we receive any request, we shall delete or otherwise destroy all of Your Protected Student Information, using the methods described above, following expiration of a 60-day period after termination of this Agreement.

5.7 We will operate the Cloud Services and collect, process and store Protected Student Information 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 Student Information, and prevent unauthorized access, disclosure and use.

5.8 We will never use Protected Student Information that we acquire through Your use of the Cloud Services for any commercial purposes, except as part of a “corporate action” (i.e., purchase, sale, merger, or other type of acquisition), if so permitted by law.

5.8.1 We will notify you if such a “corporate action” occurs. In such a case, we warrant any successor entity shall be contractually obligated to comply with the terms of this Agreement related to the treatment of Protected Student Information, as well as all other applicable legal requirements governing the use, disclosure, and security of the previously acquired Protected Student Information.

5.9 In the event of any security incident (including any actual or suspected data breach) that affects Your Data, we will follow our Information Security Policy. Unless specified in Your Order Form, or otherwise required by law, We will notify you at a time and in a manner consistent with reasonable industry standards if we detect or suspect a security incident affecting Your data occurs.

6 SUBSCRIPTION TERMS

- 6.1 Unless otherwise provided in the applicable Order Form and/or any other addenda/supplements, each Subscription Term will last for an initial 12-month period.
- 6.2 Such Agreement starts on the “Effective Date” and continues until the end of the subscription term, unless sooner terminated in accordance with these terms. If no Subscription Term is in effect, either party may terminate this Agreement for any or no reason with notice to the other party.
- 6.3 Additional offerings and/or subscriptions may be added during a subscription term, and will be prorated for the portion of that original subscription term remaining at the time the subscriptions are added. Unless otherwise indicated, any products/services added during a subscription will terminate on the same date as the preceding, underlying subscriptions.

7 FEES & PAYMENTS

- 7.1 All fees payable to Incident IQ are due within 30 days from the invoice date or as otherwise outlined in the Order Form.
- 7.2 Late payments are subject to a charge of 1.5% per month, or the maximum amount allowed by Law, whichever is less. All fees and expenses are non-refundable except as expressly set out in this Agreement.
- 7.3 You will pay any sales, value-added or other similar taxes imposed by applicable law that Incident IQ must pay based on the Cloud Services You ordered, except for taxes based on Incident IQ's income.
- 7.4 If You dispute an invoice in good faith, You will notify Us within the Payment Period and the parties will seek to resolve the dispute over a 15-day discussion period. You are not required to pay disputed amounts during the discussion period, but will timely pay all undisputed amounts. After the discussion period, either party may pursue any available remedies.
 - 7.4.1 Any such notification of dispute under 7.4 must be sent to accounting@incidentiq.com.

8 NON-INCIDENT IQ PROVIDERS

- 8.1 We or third-parties may make available Third-Party Content. Incident IQ

does not control and is not responsible for any such Third-Party Content accessible from or provided through the Cloud Services, and You bear all risks associated with any such access and use. Any Third-Party Content made accessible by Incident IQ in or through the Cloud Services is provided on an “as-is” and “as available” basis without any warranty of any kind.

- 8.2 If You choose to utilize any Third-Party Content, You grant Us permission to allow the relevant provider of such Third-Party Content to access Your Data as required for the interoperation of that Third-Party Content with the Cloud Services. We are not responsible for any disclosure, modification or deletion of Your Data resulting from access by such Third-Party Content or its provider.

9 CONFIDENTIALITY

- 9.1 By virtue of this Agreement, the parties may have access to information that is confidential to one another (“Confidential Information”). We each agree to disclose only information that is required for the performance of obligations under this Agreement or in order to comply with any governing law or binding court order.
- 9.2 Confidential information shall be limited to Your Data residing in the Cloud Services, and all information identified as confidential at the time of disclosure.
- 9.3 A party’s Confidential Information shall not include information that: (a) is or becomes a part of the public domain through no act or omission of the other party; (b) was in the other party’s lawful possession prior to the disclosure and had not been obtained by the other party either directly or indirectly from the disclosing party; (c) is lawfully disclosed to the other party by a third party without restriction on the disclosure; or (d) is independently developed by the other party. Provided, however, Student Education Records shall never not be deemed Confidential Information.
- 9.4 We each agree not to disclose each other’s Confidential Information to any third-party other than as set forth in the following sentence for a period of three (3) years from the date of the disclosing party’s disclosure of the Confidential Information to the receiving party; however, We will hold Your Confidential Information that resides within the Cloud Services in confidence for as long as such information resides in the Cloud Services.
- 9.4.1 We each may disclose Confidential Information only to those employees, agents or subcontractors who have a demonstrated need to know. Such

recipients are required to protect it against unauthorized disclosure in a manner no less protective than required under this Agreement.

9.4.2 Incident IQ will protect the confidentiality of Your Data residing in the Cloud Services in accordance with the Incident IQ security practices defined as part of Your Order Forms.

9.4.3 In addition, Your Data will be treated in accordance with the terms outlined above. Nothing shall prevent either party from disclosing Confidential Information as required by law.

9.5 In performing the Cloud Services, We will comply with the Incident IQ Privacy Policy, (available at <https://www.incidentiq.com/privacy-policy>) and incorporated herein by reference, as well as any additional requirements contained in applicable Order Forms or other documents.

9.5.1 The Incident IQ Privacy Policy is subject to change at Our discretion; however, policy changes will not result in a material reduction in the level of protection provided for Your Data during the Services Period described in Your Order Form.

9.6 We will maintain industry-standard administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of Your Data. Those safeguards will include, but will not be limited to, measures for preventing access, use, modification or disclosure of Your Data by Our personnel except (a) to provide the purchased Cloud Services and prevent or address service or technical problems, (b) as compelled by law, or (c) as You expressly permit in writing.

10 TERMINATION

10.1 In addition to any other remedies it may have, either party may also terminate this Agreement upon thirty (30) days' notice (or without notice in the case of nonpayment), if the other party materially breaches any of the terms or conditions of this Agreement or an applicable Order Form.

10.1.1 In the event we terminate for cause under 10.1 and you have not yet paid, You agree we have the right to immediately collect all sums due from You between the date of termination under 10.1 and the first day of the subscription.

10.1.2 In the event we terminate for cause under 10.1 after payment, we have full discretion on whether we will refund, whether in whole or in part, the balance of any payments made by You between the date of termination under 10.1 and the last day of the subscription.

10.2 We reserve the right to terminate any agreement at any time for any reason, or no reason at all, upon ninety (90) days' notice.

- 10.2.1 In the event we terminate under 10.2 and you have not yet paid, You agree we have the right to immediately collect all sums due from You between the date of termination following the notice period under 10.2 and the first day of the subscription.
- 10.2.2 In the event we terminate under 10.2 after payment, we will refund you the balance of any payments made by You between the date of termination and the last day of the subscription.
- 10.3 You must pay in full for the Cloud Services up to and including the last day on which the Cloud Services are provided.
- 10.4 All aspects of this Agreement which by their nature should survive termination will survive termination, including, but not limited to, accrued rights to payment, confidentiality obligations, warranty disclaimers, and limitations of liability.

11 WARRANTIES, REMEDIES AND DISCLAIMERS

- 11.1 Incident IQ warrants that it will make all reasonable efforts to perform the Cloud Services in all material respects as described in Your Order Form. If the Cloud Services provided to You were not performed as warranted, You must promptly provide written notice to Incident IQ that describes the deficiency in the Cloud Services.
- 11.2 Incident IQ does not guarantee that:
- 11.2.1 The services will be performed error-free or uninterrupted, or that Incident IQ will correct all services errors;
- 11.2.2 The services will operate in combination with your content or your applications, or with any other hardware, software, systems or data not provided by Incident IQ, and the Cloud Services will meet your requirements, specifications or expectations. You acknowledge that Incident IQ does not control the transfer of data over communications facilities, including the internet, and that the cloud services may be subject to limitations, delays, and other problems inherent in the use of such communications facilities. Neither party shall be responsible for any delays, delivery failures, or other damage resulting from such problems. Incident IQ is not responsible for any issues related to the performance, operation or security of the cloud services that arise from your data or third-party content;
- 11.2.3 Any representation or warranty regarding the reliability, accuracy, completeness, correctness, or usefulness of third-party content, and disclaims all liabilities arising from or related to third party content is true.
- 11.3 For any breach of the Cloud Services warranty, Your exclusive remedy and Incident IQ's entire liability, shall be the correction of the deficient Cloud Services that caused the breach of warranty, or, if Incident IQ

cannot substantially correct the deficiency in a commercially reasonable manner, You may end the deficient Cloud Services, and Incident IQ will refund to you the fees for the terminated services that you pre-paid to Incident IQ for the period following the effective date of termination, in a manner consistent with 10.2 above.

11.4 To the extent not prohibited by law, these warranties are exclusive and there are no other express or implied warranties or conditions including for software, hardware, systems, networks or environments or for merchantability, satisfactory quality and fitness for a particular purpose.

12 LIMITATION OF LIABILITY

1.

12.1 To the maximum extent permitted by law, each party's entire liability arising out of or related to this Agreement will not exceed the amounts paid or payable by You to US under this Agreement immediately preceding the first incident giving rise to liability."

12.2 Neither party will have any liability arising out of or related to this Agreement for indirect, special, incidental, reliance or consequential damages or damages for loss of use, lost profits or interruption of operations, even if informed of their possibility in advance.

12.3 The waivers and limitations in this Section apply regardless of the form of action, whether in contract, tort (including negligence), strict liability or otherwise and will survive and apply even if any limited remedy in this Agreement fails of its essential purpose.

13 DEFENSE & INDEMNIFICATION

13.1 We will defend You and Your employees and trustees (hereinafter and for purposes of this Section, collectively referred to as "You") against any claim, demand, suit or proceeding made or brought against You by a third-party alleging that the Cloud Services infringe or misappropriate such third-party's intellectual property rights (a "Claim Against You"), and will indemnify and hold harmless You from any damages, attorney fees and costs ultimately awarded against You as a result of, or for amounts paid by You under a settlement approved by Us in writing of, a Claim Against You.

13.1.1 In order to receive the benefit of this indemnification, you must:

13.1.1.1 promptly give Us written notice of the Claim Against You via email to legal@incidentiq.com;

13.1.1.2 give Us sole control of the defense and settlement of the Claim Against You (except that We may not settle any Claim Against You unless it unconditionally releases You of all liability); and

13.1.1.3 give Us all reasonable assistance.

13.1.2 If We receive information about an infringement or misappropriation claim related to the Cloud Services, We shall, in Our discretion and at no cost to You:

13.1.2.1 modify the Cloud Services so that they are no longer claimed to infringe or misappropriate, without breaching Our warranties described above; or

13.1.2.2 obtain a license for Your continued use of that Service in accordance with this Agreement; or

13.1.2.3 terminate Your subscriptions for the Cloud Services upon 30 days' written notice and refund You any prepaid fees covering the remainder of the term of the terminated subscriptions, consistent with 10.2 above.

13.1.3 The above defense and indemnification obligations do not apply to the extent a Claim Against You arises from Content, Third-Party Content or Your use of the Cloud Services in violation of this Agreement or applicable Order Forms; provided such Claim Against You would not have arisen but for Your use in violation of this Agreement or applicable Order Forms.

13.2 Unless otherwise prohibited by state law and/or local regulations, You will defend and indemnify Us against any claim, demand, suit or proceeding made or brought against Us by a third-party alleging that any of Your Data infringe or misappropriate such third-party's intellectual property rights, or arising from Your use of the Cloud Services or Content in violation of the Agreement, Order Forms or applicable law (each a "Claim Against Us"), and You will indemnify Us from any damages, attorney fees and costs ultimately awarded against Us as a result of, or for any amounts paid by Us under a settlement approved by You in writing of, a Claim Against Us, provided We (a) promptly give You written notice of the Claim Against Us, (b) give You sole control of the defense and settlement of the Claim Against Us (except that You may not settle any Claim Against Us unless it unconditionally releases Us of all liability), and (c) give You all reasonable assistance, at Your expense.

13.3 This Section states the indemnifying party's sole liability to, and the indemnified party's exclusive remedy against, the other party for any type of claim described in this Section.

14 MISCELLANEOUS PROVISIONS

14.1 Severability. If any provision of this Agreement is held to be invalid or unenforceable, the invalidity or unenforceability will not affect the other provisions of the Agreement.

14.2 No Waiver. A waiver of any breach of this Agreement is not deemed a waiver of any other breach.

14.3 Notices. All notices will be in writing, transmitted via certified or registered mail, postage prepaid, and delivered to the address set forth in Your Order Form. Notices may also be transmitted via e-mail and delivered to the addresses set forth in the Order Form. Notices from You to Incident IQ sent via email must be sent to legal@incidentiq.com to constitute proper notification.

14.4 Force Majeure. Neither party is liable for a delay or failure to perform this Agreement due to a Force Majeure. If a Force Majeure materially adversely affects the Cloud Service for 15 or more consecutive days, either party may terminate the affected Order(s) upon notice to the other and Provider will refund to Customer any pre-paid, unused fees for the terminated portion of the Subscription Term. However, this Section does not limit Customer's obligations to pay fees owed.

14.5 Assignment. Neither party may, without the prior written consent of the other party, assign or transfer this Agreement (or any of its rights or obligations) to any other party, except We may assign Our interests as required under any potential corporate action (i.e., acquisition, sale, merger, etc.). In the event of such a corporate action, We warrant that any successor entity will agree to abide by the terms of this agreement for the remainder of any applicable subscription term.

14.6 Relationship of the Parties. The parties are independent contractors, and no partnership, franchise, joint venture, agency, fiduciary or employment relationship between the parties is created by this Agreement.

14.7 No Third-Party Beneficiaries. There are no third-party beneficiaries to this Agreement. For clarification, even though an employee of an Affiliate may be a User under this Agreement, an Affiliate may not bring a claim against Provider arising from, based on, or under this Agreement unless such Affiliate has entered into its own Order directly with Provider.

14.8 Governing Law. **Unless prohibited by state law and/or local regulation**, this Agreement and any claims relating to its subject matter will be governed by and construed under the laws of the State of Georgia, without reference to its conflicts of law principles. All disputes

will be subject to the exclusive jurisdiction of the courts located in Fulton County, Georgia or the Federal Court of the Northern District of Georgia. Either party must initiate a cause of action for any claim(s) relating to this Agreement and its subject matter within one year from the date when the party knew, or should have known after reasonable investigation, of the facts giving rise to the claim(s).

- 14.9 Entire Agreement. This Agreement and the information which is incorporated into this Agreement by written reference (including reference to information contained in a uniform resource locator or referenced policy), together with the applicable Order Form and accompanying Exhibits, is the complete agreement for the Cloud Services ordered by You and supersedes all prior or contemporaneous agreements or representations, written or oral, regarding such Cloud Services.

SUPPORT POLICY FOR CLOUD SERVICES

1. INTRODUCTION

This Support Policy for Cloud Services ("Policy") sets forth the Support Services identified in Your applicable Order Form. The Services are governed by and subject to the terms and conditions specified in the Master Subscription Agreement and applicable Order Form signed by You (collectively the "Agreement").

2. Support Tiers

2.1. Tier One Support for Users.

2.1.1. Incident IQ Help Center. All of Your Users may access to written help documentation and video tutorials via the Cloud Services help center (located at <https://help.incidentiq.com> and through Incident IQ Academy at learn.incidentiq.com).

2.1.2. Support Request within Cloud Services Environment. All of Your Users may submit an "Incident IQ Help Ticket" using the Cloud Services. These requests first route to Your Administrator Users for resolution. If necessary Your Administrator Users may forward the request within the Cloud Services environment to the Incident IQ product support team.

2.2 Tier Two Support for Users.

2.2.1 Your Administrator Users can escalate other User help requests within the Cloud Services to the Cloud Services product support team or make such requests to the product support team directly.

2.2.2 Your Administrator Users also may access toll-free telephone support (866-899-9169) and email support (support@incidentiq.com) from the product support team during ordinary business hours (Monday through Friday, 8AM to 6PM Eastern Standard Time, excluding holidays).

3. Response Time Service Level

The Cloud Services product support team will strive to respond to support requests from Your Administrator Users within one (1) business day.

Terms of Use

Read these terms prior to accessing this Website. This Website is available for your use on the condition you agree to the terms of use presented below. By accessing the Website (defined below), you agree to be bound by the terms and conditions of this Agreement. By accessing the Website (defined below), you agree to be bound by the terms and conditions of this Agreement.

Effective Date: These Terms of Use were last updated on January 23, 2019.

- 1. Scope and Modifications.** This Agreement governs your use of the Incident IQ, LLC Online Service (the “Website”) and all applications unless certain uses or services are the subject of a separate agreement between you and Incident IQ, LLC (“Incident IQ”). By using the Website you agree to these terms and conditions. If you do not agree to the terms and conditions presented, you should immediately cease all usage of the Website. Incident IQ, at its sole discretion, reserves the right, at any time, to modify, alter, or update the terms and conditions of this Agreement without prior notice, as more fully set forth in Section 11 of this Agreement.

2. **User Eligibility.** The Website is provided by Incident IQ to be available to persons over the age of legal majority who can form legally binding agreements as provided by applicable law or to legal entities with the appropriate authority to be bound by the terms of this Agreement.
3. **Disclaimer of Warranties.** The Website, the information, the services and the content are provided by Incident IQ on an “as is” and on an “as available” basis. To the fullest extent permitted by applicable law Incident IQ makes no representations or warranties of any kind, express or implied, regarding the use or the results of this Website in terms of its correctness, accuracy, reliability, or otherwise. Incident IQ shall have no liability for any interruptions in the use of this Website. Incident IQ disclaims all warranties with regard to the information provided, including the implied warranties of merchantability and fitness for a particular purpose, and non-infringement. Some jurisdictions do not allow the exclusion of implied warranties, therefore the above-referenced exclusion may not be applicable to you.
4. **Limitation of Liability.** If you are dissatisfied with the Website or any content on the Website or do not agree to be bound by this Agreement, your sole and exclusive remedy is to discontinue using the Website. Incident IQ SHALL NOT be liable for any damages whatsoever, INCLUDING WITHOUT LIMITATION THOSE RESULTING FROM LOST PROFITS, LOST DATA, BUSINESS INTERRUPTION, LOSS OF MONEY, LOSS OF GOODWILL OR REPUTATION OR ANY INDIRECT, CONSEQUENTIAL, SPECIAL, INCIDENTAL, OR PUNITIVE DAMAGES ARISING OUT OF, BASED ON, OR RESULTING FROM THIS AGREEMENT OR USER’S USE OF THE WEBSITE OR INABILITY TO USE THE WEBSITE OR ANY

WEBSITE LINKED TO THIS WEBSITE, EVEN IF Incident IQ HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THIS FURTHER INCLUDES, BUT IS NOT LIMITED TO, DAMAGES THAT MAY RESULT FROM OMISSIONS, MISTAKES, DELETION OF FILES OR EMAILS, INTERRUPTIONS, DEFECTS, ERRORS, VIRUSES, DELAYS IN OPERATION OR TRANSMISSION, OR ANY FAILURE OF PERFORMANCE, WHETHER OR NOT RESULTING FROM ACTS OF GOD, COMMUNICATIONS FAILURE, THEFT, DESTRUCTION OR UNAUTHORIZED ACCESS TO RECORDS, PROGRAMS OR SERVICES. THESE LIMITATIONS AND EXCLUSIONS APPLY WITHOUT REGARD TO WHETHER THE DAMAGES ARISE FROM BREACH OF CONTRACT, BREACH OF WARRANTY, STRICT LIABILITY, TORT, NEGLIGENCE, OR ANY OTHER CAUSE OF ACTION, TO THE EXTENT SUCH EXCLUSION AND LIMITATIONS ARE NOT PROHIBITED BY APPLICABLE LAW.

5. **Indemnification.** You agree to indemnify, defend, and hold Incident IQ, its parents, subsidiaries, affiliates, officers and employees, harmless from any claim or demand, including reasonable attorneys' fees and costs, made by any third party due to or arising out of your use of the Website, the violation of this Agreement, or infringement by you, or other user of the Website using your computer, of any intellectual property or any other right of any person or entity.
6. **Modifications and Interruption to Service.** Incident IQ reserves the right to modify or discontinue any Website services with or without notice to you. Incident IQ shall not be liable to you or any third party should Incident IQ exercise its right to modify or discontinue a service or services provided by the Website. You acknowledge and accept that Incident IQ does not guarantee continuous, uninterrupted or secure access to its Website and

operation of its Website may be interfered with or adversely affected by numerous factors or circumstances outside of its control.

7. **Third-Party Sites.** Incident IQ may provide links to various web sites (“Third Party Sites”) not operated by Incident IQ. In addition, certain Third Party Sites also may provide links to the Incident IQ Website. These Third Party Sites are not under the control of Incident IQ. Incident IQ does not control and is not responsible or liable for any Third Party Sites or any content, advertising or other materials on or available from Third Party Sites. Incident IQ does not endorse or make any representations or give any warranties about third-party sites linked to the Website. Any links to other sites are provided merely as a convenience and, if you access any of the third-party sites linked to this Website, you do so entirely at your own risk. Incident IQ reserves the right to terminate any link or linking program at any time. You acknowledge that Incident IQ is not responsible for the availability of, data collection policies of, or the content located on or through, any third-party site. You should consult the terms of use, acceptable use policies, or other agreements of any third-party sites and should contact the site administrator or webmaster for those third-party sites if you have any concerns regarding such links or the content located on such sites. Your use of those third-party sites is subject to the terms of use and privacy policies of each site, and Incident IQ is not responsible therein.
8. **Use of Cookies.** A cookie is a text-only string of information that a website transfers to the cookie file of the browser on a user computer’s hard disk so that the website can remember who the user is. A cookie will typically contain the name of the domain

from which the cookie has come, the “lifetime” of the cookie, and a value, usually a randomly generated unique number.

When you visit the Website, Incident IQ may send a cookie to your computer. Cookies may be used in the following ways:

- To help Incident IQ recognize User as a unique visitor (just a number) when you return to the Website.
- To compile anonymous, aggregated statistics that allows Incident IQ to understand how users use the Website and to help Incident IQ improve the structure of the Website. Incident IQ cannot identify you personally in this way.

Two types of cookies may be used on this Website: (i) session cookies, which are temporary cookies that remain in the cookie file of a your browser until you leave the Website, and (ii) persistent cookies, which remain in the cookie file of your browser for much longer (though how long will depend on the lifetime of the specific cookie).

1. User Information. Your use of certain feature or registration constitutes authorization for Incident IQ to collect certain of your information, which may include, without limitation, your name, company or organization name, street address, e-mail address, telephone number, and credit card information. Incident IQ will use your information to communicate with you and for other legally permissible purposes which are necessary to provide requested services to you. Incident IQ will not sell your contact information to Internet marketing companies or sell telephone numbers to telemarketing companies.

2. Acceptable Use. You agree that when using the Website, you will not

- Violate any laws, third party rights, or Incident IQ's policies, as outlined herein or elsewhere on the Website;
- Distribute viruses, worms, Trojan horses, or any other technologies that may harm the Website, or the interests or property of Incident IQ, third party links, or other users;
- Harvest or otherwise collect information about other users, including email addresses;
- Take any action which, in Incident IQ's sole discretion, will interfere or attempt to interfere with the proper working of the Website or any activities conducted on the Website;
- Bypass any security or Website performance measures that Incident IQ implements;
- Use any robot, spider, scraper or other automated means to access the Website for any purpose without Incident IQ's express written permission;
- Reproduce the Website's content on your own website using any device including, but not limited to, use of a frame or border environment around the website, or other framing technique to enclose any portion or aspect of the Website, or mirror or replicate any portion of the Website;
- Modify, translate into any language or computer language, or create derivative works from, any content or any part of the Website;
- Reverse engineer any part of the Website; or
- Infringe the trademark or copyrights of Incident IQ.

1. **Entire Agreement.** This Agreement sets forth the entire understanding and agreement between Incident IQ and you with

respect to the subject matter hereof and supersedes any prior statements or representations. The following Sections survive any termination of this Agreement: Limitation of Liability and Intellectual Property. Incident IQ may amend this Agreement at any time by posting the amended terms on the Website. Except as stated elsewhere, all amended terms shall automatically be effective immediately after they are posted. This Agreement may not be otherwise amended except in a writing signed by User and Incident IQ.

2. Governing Jurisdiction of the Courts. This Agreement shall be governed by and interpreted in accordance with the laws of the State of Georgia, without giving effect to any choice of law rules, and shall be deemed to have been entered into in Fulton County, Georgia. The parties hereto expressly agree that any claims or disputes arising out of or in connection with this Agreement or the parties' relationship shall be brought in the Magistrate, State, or Superior Court of Fulton County, Georgia, which shall be the exclusive forum for the resolution of such claims or disputes, and the parties agree that venue over them in such Court shall be proper, and waive any objection to such venue that otherwise would be available to them.

3. Compliance with Laws. You assume all knowledge of applicable law and you are responsible for compliance with any such laws. You may not use the Website in any way that violates applicable state, federal, or international laws, regulations or other government requirements. You further agree not to transmit any material that encourages conduct that could constitute a criminal offense, give rise to civil liability or otherwise violate any applicable local, state, national, or international law or regulation.

- 4. Copyright and Trademark Information.** All content included or available on this Website, including Website design, text, graphics, interfaces, and the selection and arrangements thereof is ©2016 – 2019 Incident IQ, with all rights reserved, or is the property of Incident IQ, LLC and/or third parties protected by intellectual property rights. Any use of materials on the website, including reproduction for purposes other than those noted above, modification, distribution, or replication, any form of data extraction or data mining, or other commercial exploitation of any kind, without prior written permission of an authorized officer of Incident IQ is strictly prohibited. “Incident IQ” is a trademark of Incident IQ, LLC. The Incident IQ design is a proprietary trademark of Incident IQ, LLC. Incident IQ’s marks may not be used in connection with any product or service that is not provided by Incident IQ, in any manner that is likely to cause confusion among customers or suggest endorsement or sponsorship by Incident IQ, or in any manner that disparages or discredits Incident IQ. Other trademarks that may appear are the proprietary intellectual property of the respective owner.
- 5. Other Terms.** Each section and subsection of this Agreement constitutes a separate and distinct understanding, covenant and provision hereof. In the event that any provision of this Agreement shall finally be determined to be unlawful, such provision shall be deemed to be severed from this Agreement, but every other provision (and any partially-enforceable provision) of this Agreement shall remain in full force and effect. You agree that this Agreement and any other agreements referenced herein may be assigned by Incident IQ in our sole discretion, to a third party in the event of a merger or acquisition.



1 (877) 747-3073



Incident IQ Campus:

750 Glenwood Ave SE Suite 320
Atlanta, GA 30316

Incident IQ is a service management platform built for K-12 school districts, featuring asset management, help ticketing, human resources, facilities maintenance solutions, and more.

SITE MAP

- Home
- Getting Started
- Platform
- Success Stories
- Pricing Basics
- Company
- Student Privacy Pledge
- Careers
- Conference & Events
- Legal
- Schedule a Demo
- Contact Us

LATEST NEWS

Incident IQ to Accelerate Growth with Strategic Investment from Cove Hill Partners

February 8, 2024

Incident IQ Rolls Out an Array of User-Centric Enhancements and a Comprehensive Certification Program for K-12 Districts

November 29, 2023

What's New in Incident IQ: Jan/Feb 2024 Enhancements

February 7, 2024