monroe one
EDUCATIONAL SERVICES

Daniel T. White
District Superintendent

Lisa N. Ryan
Assistant Superintendent for Finance & Operations

TO: Members of the Board of Education
Mr. Daniel White

FROM: Lisa N. Ryan

SUBJECT: Contract Approvals

DATE: July 25, 2023

The purpose of this memo is to request that at our August 3, 2023, Board of Education meeting the Board adopt a resolution to approve the following contracts:

- Cisco – Regional Information Center – per attached
- Informed - Regional Information Center – per attached
- Securly Inc.- Regional Information Center – per attached
- Instructure - Regional Information Center – per attached
- Employee Assistance Group – Human Resources - per attached
- Genesee Community College ACE Program – Eastern Monroe Career Center – per attached

Should you have any questions please contact me prior to our August 33 meeting. Thank you.

Informed K12 AND MONROE 1 BOCES

AGREEMENT

AGREEMENT made as of April 21, 2023 by, between, and among Informed K12, having its offices at 555 12th Street, Suite 1670, Oakland, CA 94607 (hereinafter referred to as Informed K12) and The Monroe One Educational Services 41 O'Connor Road, Fairport, New York, 14450 (hereinafter referred to as "Monroe 1 BOCES"). Informed K12 enters this Agreement as an independent contractor and will remain as an independent contractor throughout the term of this agreement. Informed K12 employees shall not be entitled to any rights, payments or benefits afforded to the employees of Monroe 1 BOCES or participating school districts.

1. Scope. Informed K12 and Monroe 1 BOCES enter into affiliation solely for the purpose of offering school districts Informed K12's forms and workflow processes services. Through the affiliation, BOCES and/or participating school districts will be able to select services that they receive based on their individual/respective needs. Informed K12 will provide ongoing support and assistance to BOCES and/or participating school districts during the term of this Agreement.

2. Terms and Termination. This Agreement shall begin on April 21, 2023 and terminate on June 30, 2024; however, either of the parties may terminate this Agreement at any time and for any reason upon thirty (30) days' prior written notice to the other party. Participating school districts may elect to opt in or out of utilizing Informed K12's product and/or services at any time during the term of this Agreement.

3. Renewal. The parties may renew this Agreement by written mutual agreement sixty (60) days' prior to the end of the term.

4. Fees. The fees for services selected by BOCES and/or participating school districts during the term of this Agreement are as follows:

Participating School	License Type	Cost	Term Dates
Greece Central School District	Premium Edition: District License - Internal	$51,912	07/03/2023 – 07/02/2024

BOCES and/or participating school districts will be invoiced for the services selected. In the event of early termination of services by a participating school district, Informed K12 will reimburse the fees to BOCES and/or the participating school district on a *pro rata* monthly basis.

5. Indemnification. Each party agrees to indemnify and hold each other and each of their officers, directors, employees agents and assigns, harmless from and against all claims, causes of action, damages, liabilities, fines, costs and expenses (including reasonable attorneys' fees) that may arise from the violation of the terms of this Agreement, violation of any applicable laws, infringement of third party proprietary and/or intellectual property rights, libel, slander and other torts including with respect to personal injury, property damage and death arising from the negligent or willfully wrongful acts or omissions of its employees, third-party vendors, contractors, subcontractors or agents, in connection with the services provided in connection with this Agreement.

6. Cooperation. The parties agree to cooperate with each other in connection with any internal investigations by Informed K12 or Monroe 1 BOCES of possible violation of their respective policies and procedures and any third-party litigation.

7. Confidentiality. Informed K12 agrees that any and all data obtained from Monroe 1 BOCES and/or a participating school district shall be used expressly and solely for the purposes enumerated in this Agreement. Monroe 1 BOCES data and participating school district data shall not be distributed, used, or shared for any other purpose. Informed K12 shall not sell, transfer, share or process any Monroe 1 BOCES data or participating school district data for any purpose other than those under this Agreement, including commercial advertising, marketing, or any other commercial purpose. Informed K12 will comply with the terms and conditions set forth in the Education Law Section 2-d Contract Addendum, which is attached hereto as **Appendix A** and is incorporated by reference as if fully set forth herein. Informed K12 shall comply with all applicable laws, rules and regulations, including, but not limited to the Family Educational Rights and Privacy Act and New York Education Law Section 2-d and its implementing regulations.

8. Independent Contractor: This Agreement does not create an employee/employer relationship between the parties or between Informed K12 and any participating school district. Informed K12 will be an independent contractor and not a Monroe 1 BOCES or school district employee for any purpose whatsoever. No Informed K12 employee shall be entitled to any payment or benefit from Monroe 1 BOCES or a participating school district.

9. Non-Discrimination and Legal Compliance. Informed K12 agrees that it will not discriminate against anyone with respect to the provision of services hereunder on the grounds of race, religion, creed, color, national origin, gender, sexual orientation, disability, marital status, veteran status or other protected category. In providing the services pursuant to this Agreement, Informed K12 will comply with all applicable laws, rules and regulations.

11. Jurisdiction. This Agreement shall be governed by the laws of the State of New York. Litigation of all disputes between the parties arising from or in connection with this Agreement shall be conducted in a court of appropriate jurisdiction in the State of New York, County of Monroe, New York.

12. Insurance. Each party hereby agrees to obtain and thereafter maintain in full force and effect during the term of this Agreement general liability insurance with limits not less than $1,000,000 per occurrence and $2,000,000 annual aggregate.

13. **Order of Interpretation and Control.** In the event of a conflict between this Agreement, the Education Law Section 2-d Contract Addendum (Appendix A), or any other document, the Education Law Section 2-d Contract Addendum (Appendix A) shall control, and then this Agreement. Informed K12 shall not include any term in any such form or format that contradicts the terms to which it has agreed in this Agreement or with Education Law Section 2-d.

14. **Notices.** All notices to Informed K12 and Monroe 1 BOCES in connection with this Agreement shall be sent to:

Jennifer Bundy
Head of Finance & Operations
Informed K12
operations@informedk12.com

All notices to Monroe 1 BOCES in connection with this Agreement shall be sent to:
Lisa N. Ryan
Assistant Superintendent for Finance & Operations
Monroe 1 BOCES
41 O'Connor Road
Fairport, NY 14450

15. **Entire Agreement**. This Agreement and Appendix A constitute the entire agreement between the parties.

IN WITNESS WHEREOF, the parties hereto have executed this Agreement as of the day and year first above written.

Informed K12, Inc.

By: Jennifer Bundy

Jennifer Bundy

Head of Finance & Operations

THE MONROE 1 BOARD OF COOPERATIVE EDUCATIONAL SERVICES

By:

Daniel T. White

District Superintendent

Appendix A
Compliance With New York State Education Law Section 2-d Addendum ("Addendum")

The parties to this Agreement are the Monroe 1 Board of Cooperative Educational Services ("BOCES") and Informed K12, Inc. ("Vendor"). BOCES is an educational agency, as that term is used in Section 2-d of the New York State Education Law ("Section 2-d") and its implementing regulations, and Vendor is a third party contractor, as that term is used in Section 2-d and its implementing regulations. BOCES and Vendor have entered into this Agreement to conform to the requirements of Section 2-d and its implementing regulations. To the extent that any term of any other agreement or document conflicts with the terms of this Agreement, the terms of this Agreement shall apply and be given effect.

Definitions
As used in this Agreement and related documents, the following terms shall have the following meanings:
"Student Data" means personally identifiable information from student records that Vendor receives from an educational agency (including BOCES or a Participating School District) in connection with providing Services under this Agreement.
"Personally Identifiable Information" ("PII") as applied to Student Data, means personally identifiable information as defined in 34 CFR 99.3 implementing the Family Educational Rights and Privacy Act (FERPA), at 20 USC 1232g.
"Third Party Contractor," "Contractor" or "Vendor" means any person or entity, other than an educational agency, that receives Student Data from an educational agency pursuant to a contract or other written agreement for purposes of providing services to such educational agency, including, but not limited to data management or storage services, conducting studies for or on behalf of such educational agency, or audit or evaluation of publicly funded programs.
"BOCES" means Monroe #1 Board of Cooperative Educational Services.
"Parent" means a parent, legal guardian, or person in parental relation to a student.
"Student" means any person attending or seeking to enroll in an educational agency.
"Eligible Student" means a student eighteen years or older.
"State-protected Data" means Student Data, as applicable to Vendor's product/service.
"Participating School District" means a public school district or board of cooperative educational services that obtains access to Vendor's product/service through a cooperative educational services agreement ("CoSer") with BOCES, or other entity that obtains access to Vendor's product/service through an agreement with BOCES, and also includes BOCES when it uses the Vendor's product/service to support its own educational programs or operations.
"Breach" means the unauthorized access, use, or disclosure of personally identifiable information.
"Commercial or marketing purpose" means the sale of PII; and the direct or indirect use or disclosure of State-protected Data to derive a profit, advertise, or develop, improve, or market products or services to students other than as may be expressly authorized by the parties in writing (the "Services").
"Disclose", "Disclosure," and "Release" mean to intentionally or unintentionally permit access to State-protected Data; and to intentionally or unintentionally release, transfer, or otherwise communicate State-protected Data to someone not authorized by contract, consent, or law to receive that State-protected Data.

Vendor Obligations and Agreements

Vendor agrees that it shall comply with the following obligations with respect to any student data received in connection with providing Services under this Agreement and any failure to fulfill one of these statutory or regulatory obligations shall be a breach of this Agreement. Vendor shall:

(a) limit internal access to education records only to those employees and subcontractors that are determined to have legitimate educational interests in accessing the data within the meaning of Section 2-d, its implementing regulations and FERPA (e.g., the individual needs access in order to fulfill his/her responsibilities in providing the contracted services);

(b) only use personally identifiable information for the explicit purpose authorized by the Agreement, and must/will not use it for any purpose other than that explicitly authorized in the Agreement or by the parties in writing;

(c) not disclose any personally identifiable information received from BOCES or a Participating School District to any other party who is not an authorized representative of the Vendor using the information to carry out Vendor's obligations under this Agreement, unless (i) if student PII, the Vendor or that other party has obtained the prior written consent of the parent or eligible student, or (ii) the disclosure is required by statute or court order, and notice of the disclosure is provided to the source of the information no later than the time of disclosure, unless such notice is expressly prohibited by the statute or court order;

(d) maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of the personally identifiable information in its custody;

(e) use encryption technology to protect data while in motion or in its custody (i.e., in rest) from unauthorized disclosure by rendering personally identifiable information unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified or permitted by the Secretary of the United States department of health and human services in guidance issued under Section 13402(H)(2) of Public Law 111-5 using a technology or methodology specified or permitted by the secretary of the U S.);

(f) not sell personally identifiable information received from BOCES or a Participating School District nor use or disclose it for any marketing or commercial purpose unless otherwise expressly authorized by the Services, or facilitate its use or disclosure by any other party for any marketing or commercial purpose or permit another party to do so;

(g) notify the educational agency from which student data is received of any breach of security resulting in an unauthorized release of such data by Vendor or its assignees in violation of state or federal law, or of contractual obligations relating to data privacy and security in the most expedient way possible and without unreasonable delay, in compliance with New York law and regulation;

(h) reasonably cooperate with educational agencies and law enforcement to protect the integrity of investigations into any breach or unauthorized release of personally identifiable information by Vendor;

(i) adopt technologies, safeguards, and practices that align with the NIST Cybersecurity Framework, Version 1.1, that are in substantial compliance with the BOCES data security and privacy policy, and that comply with Education Law Section 2-d, Part 121 of the Regulations of the Commissioner of Education and the Monroe #1 BOCES Parents' Bill of Rights for Data Privacy and Security, set forth below, as well as all applicable federal, state and local laws, rules and regulations;

(j) acknowledge and hereby agrees that the State-protected Data which Vendor receives or has access to pursuant to this Agreement may originate from several Participating School Districts located across New York State. Vendor acknowledges that the State-protected Data belongs to and is owned by the Participating School District or student from which it originates;

(k) acknowledge and hereby agrees that if Vendor has an online terms of service and/or Privacy Policy that may be applicable to its customers or users of its product/service, to the extent that any term of such online terms of service or Privacy Policy conflicts with applicable law or regulation, the terms of the applicable law or regulation shall apply;

(l) acknowledge and hereby agrees that Vendor shall promptly pay for or reimburse the educational agency for the full third party cost of a legally required breach notification to parents and eligible students due to the unauthorized release of student data caused by Vendor or its agent or assignee;

(m) ensure that employees, assignees and agents of Contractor who have access to student data, or teacher or principal data receive or will receive training on the federal and state laws governing confidentiality of such data prior to receiving access to such data; and

(n) ensure that any subcontractor that performs Contractor's obligations pursuant to the Agreement is legally bound by legally compliant data protection obligations imposed on the Contractor by law, the Agreement and this Agreement.

Monroe #1 BOCES Parents' Bill of Rights for Data Privacy and Security
(https://www.monroe.edu/domain/1478)

The Monroe #1 BOCES seeks to use current technology, including electronic storage, retrieval, and analysis of information about students' education experience in the BOCES, to enhance the opportunities for learning and to increase the efficiency of our operations.

The Monroe #1 BOCES seeks to ensure that parents have information about how the BOCES stores, retrieves, and uses information about students, and to meet all legal requirements for maintaining the privacy and security of protected student data and protected principal and teacher data, including Section 2-d of the New York State Education Law.

To further these goals, the BOCES has posted this Parents' Bill of Rights for Data Privacy and Security.

1. A student's personally identifiable information cannot be sold or released for any commercial purposes.
2. Parents have the right to inspect and review the complete contents of their child's education record. The procedures for exercising this right can be found in Student Records Policy 6320. (https://www.monroe.edu/6320)
3. State and federal laws protect the confidentiality of personally identifiable information, and safeguards associated with industry standards and best practices, including but not limited to, encryption, firewalls, and password protection, must be in place when data is stored or transferred.
4. A complete list of all student data elements collected by the State is available at http://www.p12.nysed.gov/irs/sirs/documentation/NYSEDstudentData.xlsx and a copy may be obtained by writing to the Office of Information & Reporting Services, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, New York 12234.
5. Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed in writing, to:

   Chief Privacy Officer
   New York State Education Department
   Room 863 EBA
   89 Washington Avenue
   Albany, New York 12234.

   or
   Monroe One Data Protection Officer
   William Gregory
   Monroe #1 BOCES
   41 O'Connor Road
   Fairport, NY 14450

Supplemental Information About Agreement Between Informed K12 and BOCES

(a) The exclusive purposes for which the personally identifiable information provided by BOCES or a Participating School District will be used by Vendor is to provide Informed K12's forms and workflow processes services to BOCES or other Participating School District pursuant to a BOCES Purchase Order.

(b) Personally identifiable information received by Vendor, or by any assignee of Vendor, from BOCES or from a Participating School District shall not be sold or used for marketing purposes.

(c) Personally identifiable information received by Vendor, or by any assignee of Vendor shall not be shared with a sub-contractor except pursuant to a written contract that binds such a party to at least the same data protection and security requirements imposed on Vendor under this Agreement, as well as all applicable state and federal laws and regulations.

(d) The effective date of this Agreement shall be April 21, 2023 and the Agreement shall remain in effect until June 30, 2024, unless sooner by either party for any reason upon thirty (30) days' notice.

(e) Upon expiration or termination of the Agreement without a successor or renewal agreement in place, and upon request from BOCES or a Participating School District, Vendor shall transfer all educational agency data to the educational agency in a format agreed upon by the parties. Vendor shall thereafter securely delete all educational agency data remaining in the possession of Vendor or its assignees or subcontractors (including all hard copies, archived copies, electronic versions or electronic imaging of hard copies) as well as any and all educational agency data maintained on behalf of Vendor in secure data center facilities, other than any data that Vendor is required to maintain pursuant to law, regulation or audit requirements. Vendor shall ensure that no copy, summary or extract of the educational agency data or any related work papers are retained on any storage medium whatsoever by Vendor, its subcontractors or assignees, or the secure data center facilities unless Vendor is required to keep such data for legal, regulator, or audit purposes, in which case the data will be retained in compliance with the terms of this Agreement. To the extent that Vendor and/or its subcontractors or assignees may continue to be in possession of any de-identified data (data that has had all direct and indirect identifiers permanently removed with no possibility of reidentification), they each agree not to attempt to re-identify de-identified data and not to transfer de-identified data to any party. Upon request, Vendor and/or its subcontractors or assignees will provide a certification to the BOCES or Participating School District from an appropriate officer that the requirements of this paragraph have been satisfied in full.

(f) State and federal laws require educational agencies to establish processes for a parent or eligible student to challenge the accuracy of their student data. Third party contractors must cooperate with educational agencies in complying with the law. If a parent or eligible student submits a challenge to the accuracy of student data to the student's district of enrollment and the challenge is upheld, Vendor will cooperate with the educational agency to amend such data.

(g) Vendor shall store and maintain PII in electronic format on systems maintained by Vendor in a secure data center facility in the United States in accordance with its Privacy Policy, NIST Cybersecurity Framework, Version 1.1, and the BOCES data security and privacy policy, Education Law Section 2-d, Part 121 of the Regulations of the Commissioner of Education, and the Monroe #1 BOCES Parents' Bill of Rights for Data Privacy and Security, set forth above. Encryption technology will be utilized while data is in motion and at rest, as detailed above.

(h) A copy of Vendor's Data Privacy and Security Plan, which vender affirms complies with 8 N.Y.C.R.R. 121.6 is attached hereto as **Attachment 1** and is incorporated herein by reference as if fully set forth herein.

Jennifer Bundy — 05/04/2023

Vendor Signature — Date

ATTACHMENT 1 - CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

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

1	Outline how you will implement applicable data security and privacy contract requirements over the life of the Contract.	The Informed K12 platform is hosted on Heroku, a service that relies on Amazon Web Services. Heroku utilizes SOC-2, ISO 27001 and FISMA certified data centers managed by Amazon. We have also completed the NIST Framework for districts we work with in New York.
2	Specify the administrative, operational, and technical safeguards and practices that you have in place to protect PII.	Informed K12 uses physical, managerial, and technical safeguards to help preserve the integrity and security of data entered into the system. These safeguards include, but are not limited to, third party data center operations accredited under ISO 27001 and other security assessments, password-protected accounts, access to user accounts by authorized Informed K12 staff only for the purposes of supporting the account, data encryption in transit and at rest, and technical separations between data sets.
3	Address the training received by your employees and any subcontractors engaged in the provision of services under the Contract on the federal and state laws that govern the confidentiality of PII.	All Informed K12 employees go through a background check and reference checks. All new employees go through security training within their first 30 days of employment. During onboarding, employees set up security safeguards such as two-factor authentication on sensitive systems. The Informed K12 operations team conducts company-wide security and

		data privacy refresher trainings throughout the year.
4	Outline contracting processes that ensure that your employees and any subcontractors are bound by written agreement to the requirements of the Contract, at a minimum.	All employees sign a confidentiality agreement, employee handbook policies, and undergo training around contracts and data privacy and security practices. All subcontractor contracts are reviewed by the Operations department for the inclusion of terms that align with the requirements of the Contract.
5	Specify how you will manage any data security and privacy incidents that implicate PII and describe any specific plans you have in place to identify breaches and/or unauthorized disclosures, and to meet your obligations to report incidents to the EA.	Immediately upon becoming aware of a compromise of District Confidential Information and/or PII, or of circumstance that could have resulted in unauthorized access to or disclosure or use of District Confidential Information, Company will notify District, fully investigate the incident, and cooperate fully with District's investigation of and response to the incident. Except as otherwise required by law, Company will not provide notice of the incident directly to the persons whose data were involved, regulatory agencies, or other entities, without prior written permission from District.
6	Describe how data will be transitioned to the EA when no longer needed by you to meet your contractual obligations, if applicable.	Data ownership for district data is addressed in Informed K12's Terms of Service and Privacy Policy. Districts retain ownership of their data. Upon contract termination, this data can be downloaded from our system by the district and deleted from our servers.
7	Describe your secure destruction practices and how certification will be provided to the EA.	Informed K12 will regularly backup district data and retain such backup copies for the duration of the Agreement term. At the end of the term, Informed K12 will notify the designated district administrator of the 30-day data retention period. Informed K12 will retain data for 30 days so that the district can download any data that needs to be retained. After 30 days, or

		upon request by the district, all district-owned data in district accounts will be destroyed and is no longer accessible. Districts may request data from a specific form be removed at any time during the agreement through a designated school administrator. After data destruction, the requesting party will receive email confirmation that data has been permanently deleted and is no longer accessible.
8	Outline how your data security and privacy program/practices align with the EA's applicable policies.	The District retains ownership over data; the district point person with Informed K12 can request data deletion with their account manager. Informed K12 staff directs individuals to your district point person for anyone requesting information from a submitted form. Data is encrypted in transit and at rest. These data centers are accredited under ISO 27001, SOC 1 and SOC 2/SSAE16/ISAE 3402, PCI Level 1, FISMA Moderate, Sarbanes-Oxley Forms sent directly via email are not accessible outside of email unless link is shared. These emails do not impersonate the district; they are sent from the sender via Informed K12. An audit trail within product indicates when the form is signed, by whom, and when.
9	Outline how your data security and privacy program/practices materially align with the NIST CSF v1.1 using the Framework chart below.	PLEASE USE TEMPLATE BELOW.

ATTACHMENT 1(A) – NIST CSF TABLE

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

Function	Category	Contractor Response
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	All employees are issued Apple laptop computers that are managed by a third-party consultant that supports IT and data security and privacy initiatives. Devices are able to be remotely wiped and are kept updated with antivirus and malware protection. Informed K12 uses Google Apps to manage employee email and file storage accounts; all employees are required to have two-factor authentication on their Google and Informed K12 accounts. The service that runs the Informed K12 platform is managed by Heroku, a secure, industry leading application platform. Heroku is a cloud application platform used by organizations of all sizes to deploy and operate applications throughout the world. The platform allows organizations to focus on application development and business strategy while Heroku focuses on infrastructure management, scaling, and security. Heroku applies security best practices and manages platform security so customers can focus on their business. The platform is designed to protect customers from threats by applying security controls at every layer from physical to application, isolating customer applications and data, and with its ability to rapidly deploy security updates without customer interaction or service interruption. More details at https://www.heroku.com/policy/security
	Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	Informed K12 currently works with K-12 school districts and schools, supporting them in increasing operational efficiency through workflow automation with forms. Each district partner has a dedicated team that consists of a District Partnerships Account Executive and a Customer Success Manager (CSM), in addition to technical and customer support teams. The CSMs are responsible for maintaining primary contacts at the district that have authority to make decisions around district data and processes. The roles of the Informed K12 employee determines the level of access they have to district data and their responsibilities in relation to data security and privacy and risk management decisions.
	Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	Informed K12 has laid out policies, procedures, and processes that monitor operational requirements and cybersecurity risk. Our CTO has explored best practices for esignature providers and employed those practices internally. As needed, the company contracts third party vendors and advisors that specialize in data security and privacy to define and update internal processes and procedures in the changing regulatory environment.

Function	Category	Contractor Response
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	Informed K12 is aware of cybersecurity risk to organizational operations, organizational assets, and individuals due to the nature of the type of data potentially being captured on the platform by districts. We work closely with all district partners to consult on the type of data they might be collecting via electronic forms and any risk might be associated with the data.
	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	Informed K12 has established priorities, constraints, risk tolerances, and assumptions in the creation and execution of operational risk decisions. In relation to district data, districts own their processes and data, and make the sole decisions as to who at the district has the authority to make operational risk decisions on behalf of the district. Informed K12 provides districts with the relevant information about the platform and its data security and privacy standards in order for districts to make such decisions.
	Supply Chain Risk Management (ID.SC): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.	Informed K12 utilizes data platforms commonly used by SaaS businesses to provide services, such as Amazon Web Services and Heroku. Informed K12 has a process for reviewing third party contracts that involves multiple people reviewing the contract for terms and conditions. Third party vendors are vetted for the types of data they will have access to and for adherence to federal and state regulations in how they handle data privacy and security.
PROTECT (PR)	**Identity Management, Authentication and Access Control (PR.AC):** Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	The physical location of Informed K12 is limited by daily security and key card access to the office building. Any and all equipment that might connect to platform data is either kept in a locked cabinet or remains in the possession of employees. All laptop equipment can be remotely wiped. The Informed K12 platform is hosted on Heroku, a service that relies on Amazon Web Services. Heroku utilizes ISO 27001 and FISMA certified data centers managed by Amazon. Amazon has many years of experience in designing, constructing, and operating large-scale data centers. This experience has been applied to the AWS platform and infrastructure. AWS data centers are housed in nondescript facilities, and critical facilities have extensive setback and military grade perimeter control berms as well as other natural boundary protection. Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, state-of-the-art intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication no fewer than three times to access data center floors. All visitors and contractors are required to present identification and are signed in and continually escorted by authorized staff. Amazon only provides data center access and information to employees who have a legitimate business need for such

Function	Category	Contractor Response
		privileges. When an employee no longer has a business need for these privileges, his or her access is immediately revoked, even if they continue to be an employee of Amazon or Amazon Web Services. All physical and electronic access to data centers by Amazon employees is logged and audited routinely. More details at https://www.heroku.com/policy/security
	Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.	Employees undergo data security and privacy training prior to having any access to district owned data. Informed K12 provides training on data security and privacy policies on at least an annual basis. Informed K12 training has been developed in collaboration with third party consultants that specialize in data privacy and security with K-12 public school districts. All employees are trained to follow specific policies and procedures in the event of a perceived data compromise and have access to customer agreements that indicate any terms around data privacy and security.
	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	The Informed K12 platform is hosted on Heroku, a service that provides the following data security: Each application on the Heroku platform runs within its own isolated environment and cannot interact with other applications or areas of the system. This restrictive operating environment is designed to prevent security and stability issues. These self-contained environments isolate processes, memory, and the file system using LXC while host-based firewalls restrict applications from establishing local network connections. For additional technical information see: https://devcenter.heroku.com/articles/dyno-isolation Informed K12's platform data is stored in the "Heroku Postgres" database system. Under that system, customer data is stored in separate access-controlled databases per application. Each database requires a unique username and password that is only valid for that specific database and is unique to a single application. Customers with multiple applications and databases are assigned separate databases and accounts per application to mitigate the risk of unauthorized access between applications. Customer connections to postgres databases require SSL encryption to ensure a high level of security and privacy. More details at https://www.heroku.com/policy/security

Function	Category	Contractor Response
	Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	Informed K12 has internal policies that determine access and responsibilities for data systems and assets based on role. Employees that are not directly supporting customers in monitoring and maintaining online workflows and forms do not have access to platform data. Regardless of access, all employees undergo training on reporting perceived threats or data compromises and on processes and policies for data or security breaches.
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	Informed K12 is hosted on the Heroku Platform. Under Heroku system configuration and consistency is maintained through standard, up-to-date images, configuration management software, and by replacing systems with updated deployments. Systems are deployed using up-to-date images that are updated with configuration changes and security updates before deployment. Once deployed, existing systems are decommissioned and replaced with up-to-date systems. More details at https://www.heroku.com/policy/security
	Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	Informed K12 is hosted on the Heroku platform that provides industry leading protection to any physical assets. Additionally the running application code has security through the Heroku platform's design. The design of the Heroku platform is explicitly designed to provide security as well as resiliency of the Informed K12 platform. More details at https://www.heroku.com/policy/security All employees also have antivirus and malware detectors installed and running on computers and two-factor authentication for applications that have access to sensitive data where two-factor authentication is available, including but not limited to Google Apps and product email logs.
DETECT (DE)	**Anomalies and Events (DE.AE):** Anomalous activity is detected and the potential impact of events is understood.	Informed K12 utilizes several tools that both alert about anomalous activity as well as provide data if forensic investigation is required. LogDNA is used to track all activity on the platform and as well as alert us when specified errors or non-standard activities occur. The service tracks all activity on the service, and all LogDNA plans are compliant with SOC 2 Type 2, PCI-DSS, GDPR, EU-US Privacy Shield, and CCPA. more details https://www.logdna.com/security Honeybadger is a service used to record the details about errors on the platform, as well as alert us when certain errors and

Function	Category	Contractor Response
		non-standard activities occur. Honeybadger has achieved SOC 2 Type 1 Compliance as well as GDPR compliance. More details https://www.honeybadger.io/security/
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	Informed K12 conducts annual penetration testing events to verify the effectiveness of their application design as well as the related systems the platform relies on.
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	Informed K12 has notification processes and systems that are continually reviewed and adjusted to ensure they are set to the correct thresholds of our platform.
RESPOND (RS)	**Response Planning (RS.RP):** Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.	The Informed K12 engineering team has a weekly rotation with redundancies to ensure that a qualified engineer is always available and responsible for monitoring the state of the systems and security notifications and responding if an incident is detected.
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	The Informed K12 Customer Success Manager coordinates any necessary response to compromised data in collaboration with the primary district contact. Informed K12 will not contact the individual affected directly, without approval from the district partner. The district is responsible for determining any necessary notifications as needed. Informed K12 will support the district in delivering any necessary notifications as desired.
	Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.	Analysis of any incident is done using observation tools: LogDNA and Honeybadger. Both offer real-time access to activity on the platform and persist their data to allow for forensic research for events up to 30 days. The combination of tools allows Informed K12 to review issues on the platform through different perspectives to better investigate any issues.
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	In the case Informed K12 is notified in any way about an incident on the platform, there are several tools in place that allow us to immediately lock the system down to prevent damage. • Heroku provides all applications on its platform the ability to deny any access to the platform with the click of a button while still allowing us access to all of our forensic tools • The Informed K12 application has a view-only mode as a way to prevent any data from being changed, while still allowing platform users to view their data
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	Informed K12 maintains an internal log of data compromises and any lessons learned from detection and response activities are immediately implemented into team practices, processes, and policies.

Function	Category	Contractor Response
RECOVER (RC)	**Recovery Planning (RC.RP):** Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.	Data on the Informed K12 platform is hosted in a Heroku Postgres database. This service uses Continuous Protection to keep data safe on Heroku Postgres. Every change to the data is written to write-ahead logs, which are shipped to multi-datacenter, high-durability storage. In the unlikely event of unrecoverable hardware failure, these logs can be automatically 'replayed' to recover the database to within seconds of its last known state. Completing this process requires the platform to go offline for ~20 minutes, so it is not scheduled unless necessary, however,we maintain explicit internal documentation on how to schedule, communicate and complete the recovery. For additional technical information see: https://devcenter.heroku.com/articles/pgbackups Code used to run the Informed K12 platform is hosted in Github, a world leader in source code management. In the case of an issue, the history of our codebase is visible to examine and changes are able to be quickly undone. The complete history of every change and author is immediately available. Informed K12 is hosted on the Heroku platform which combined with our Github use, allows us to immediately undo any changes in the production application via a "roll back" process. This process is well tested and happens within minutes of initiation. This rollback process is tested twice a year.
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	After any incident the Informed K12 team goes through a "Five Whys" retrospective to ensure that the root cause of the issue is well understood by all, and effective remediations can be put in place to prevent the specific issue from happening again due to the same reasons. Any adjustments to processes are documented in internal documentation.
	Communications (RC.CO): Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).	The Informed K12 Customer Success Manager coordinates communications in collaboration with the primary district contact. Informed K12 manages any restoration activities with third party vendors directly. Access to any data for district staff is reinstated in coordination with the district. Informed K12 will work with the district to coordinate response communication and obligations for any individuals affected.