Code 45

Educational
Technology Service
Genesee Valley
Wayne-Finger Lakes

EDUTECH

**CONTRACT ADDENDUM**

**Protection of Student Personally Identifiable Information**

**1. Applicability of This Addendum**

The Wayne-Finger Lakes BOCES/EduTech) and CodeHS, **("Vendor")** are parties to a contract dated 7/1/2023 ("the underlying contract") governing the terms under which BOCES accesses, and Vendor provides, web-based plpl ("Product"). Wayne-Finger Lakes BOCES/EduTech use of the Product results in Vendor receiving student personally identifiable information as defined in New York Education Law Section 2-d and this Addendum. The terms of this Addendum shall amend and modify the underlying contract and shall have precedence over terms set forth in the underlying contract and any online Terms of Use or Service published by Vendor.

**2. Definitions**

2.1. "Protected Information", as applied to student data, means "personally identifiable information" as defined in 34 CFR Section 99.3 implementing the Family Educational Rights and Privacy Act (FERPA) where that information is received by Vendor from BOCES or is created by the Vendor's product or service in the course of being used by BOCES.

2.2. "Vendor" means CodeHS, Inc.

2.3. "Educational Agency" means a school BOCES, board of cooperative educational services, school, or the New York State Education Department; and for purposes of this Contract specifically includes Wayne-Finger Lakes BOCES/EduTech.

2.4. "BOCES" means the Wayne-Finger Lakes BOCES/EduTech.

2.5. "Parent" means a parent, legal guardian, or person in parental relation to a Student.

2.6. "Student" means any person attending or seeking to enroll in an educational agency.

2.7. "Eligible Student" means a student eighteen years or older.

2.8. "Assignee" and "Subcontractor" shall each mean any person or entity that receives, stores, or processes Protected Information covered by this Contract from Vendor for the purpose of enabling or assisting Vendor to deliver the product or services covered by this Contract.

2.9. "This Contract" means the underlying contract as modified by this Addendum.

**3. Vendor Status**

Vendor acknowledges that for purposes of New York State Education Law Section 2-d it is a third-party contractor, and that for purposes of any Protected Information that constitutes education records under the Family Educational Rights and Privacy Act (FERPA) it is a school official with a legitimate educational interest in the educational records.

**4. Confidentiality of Protected Information**

Vendor agrees that the confidentiality of Protected Information that it receives, processes, or stores will be handled in accordance with all state and federal laws that protect the confidentiality of Protected Information, and in accordance with the BOCES Policy on Data Security and Privacy, a copy of which is Attachment B to this Addendum.

**5. Vendor Employee Training**

Vendor agrees that any of its officers or employees, and any officers or employees of any Assignee of Vendor, who have access to Protected Information will receive training on the federal and state law governing confidentiality of such information prior to receiving access to that information.

**6. No Use of Protected Information for Commercial or Marketing Purposes**

Vendor warrants that Protected Information received by Vendor from BOCES or by any Assignee of Vendor, shall not be sold or used for any commercial or marketing purposes; shall not be used by Vendor or its Assignees for purposes of receiving remuneration, directly or indirectly; shall not be used by Vendor or its Assignees for advertising purposes; shall not be used by Vendor or its Assignees to develop or improve a product or service; and shall not be used by Vendor or its Assignees to market products or services to students.

**7. Ownership and Location of Protected Information**

7.1. Ownership of all Protected Information that is disclosed to or held by Vendor shall remain with BOCES. Vendor shall acquire no ownership interest in education records or Protected Information.

7.2. BOCES shall have access to the BOCES's Protected Information at all times through the term of this Contract. BOCES shall have the right to import or export Protected Information in piecemeal or in its entirety at their discretion, without interference from Vendor.

7.3. Vendor is prohibited from data mining, cross tabulating, and monitoring data usage and access by BOCES or its authorized users, or performing any other data analytics other than those required to provide the Product to BOCES. Vendor is allowed to perform industry standard back-ups of Protected Information. Documentation of back-up must be provided to BOCES upon request.

7.4. All Protected Information shall remain in the continental United States (CONUS) or Canada. Any Protected Information stored, or acted upon, must be located solely in data centers in CONUS or Canada. Services which directly or indirectly access Protected Information may only be performed from locations within CONUS or Canada. All helpdesk, online, and support services which access any Protected Information must be performed from within CONUS or Canada.

**8. Purpose for Sharing Protected Information**

The exclusive purpose for which Vendor is being provided access to Protected Information is to provide the product or services that are the subject of this Contract to Wayne-Finger Lakes BOCES/EduTech.

**9. Downstream Protections**

Vendor agrees that, in the event that Vendor subcontracts with or otherwise engages another entity in order to fulfill its obligations under this Contract, including the purchase, lease, or sharing of server space owned by another entity, that entity shall be deemed to be an "Assignee" of Vendor for purposes of Education Law Section 2-d, and Vendor will only share Protected Information with such entities if those entities are contractually bound to observe the same obligations to maintain the privacy and security of Protected Information as are required of Vendor under this Contract and all applicable New York State and federal laws.

**10. Protected Information and Contract Termination**

10.1. The expiration date of this Contract is defined by the underlying contract.

10.2. Upon expiration of this Contract without a successor agreement in place, Vendor shall assist BOCES in exporting all Protected Information previously received from, or then owned by, BOCES.

10.3. Vendor shall thereafter securely delete and overwrite any and all Protected Information 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 of shared data) as well as any and all Protected Information maintained on behalf of Vendor in secure data center facilities.

10.4. Vendor shall ensure that no copy, summary or extract of the Protected Information or any related work papers are retained on any storage medium whatsoever by Vendor, its subcontractors or assignees, or the aforementioned secure data center facilities.

10.5. 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 removed) derived from Protected Information, they agree not to attempt to re-identify de-identified data and not to transfer de-identified data to any party.

10.6. Upon request, Vendor and/or its subcontractors or assignees will provide a certification to BOCES from an appropriate officer that the requirements of this paragraph have been satisfied in full.

**11. Data Subject Request to Amend Protected Information**

11.1. In the event that a parent, student, or eligible student wishes to challenge the accuracy of Protected Information that qualifies as student data for purposes of Education Law Section 2-d, that challenge shall be processed through the procedures provided by the BOCES for amendment of education records under the Family Educational Rights and Privacy Act (FERPA).

11.2. Vendor will cooperate with BOCES in retrieving and revising Protected Information, but shall not be responsible for responding directly to the data subject.

**12. Vendor Data Security and Privacy Plan**

12.1. Vendor agrees that for the life of this Contract the Vendor will maintain the administrative, technical, and physical safeguards described in the Data Security and Privacy Plan set forth in Attachment C to this Contract and made a part of this Contract.

12.2. Vendor warrants that the conditions, measures, and practices described in the Vendor's Data Security and Privacy Plan:

12.3. align with the NIST Cybersecurity Framework 1.0;

12.4. equal industry best practices including, but not necessarily limited to, disk encryption, file encryption, firewalls, and password protection;

12.5. outline how the Vendor will implement all state, federal, and local data security and privacy contract requirements over the life of the contract, consistent with the BOCES data security and privacy policy (Attachment B);

12.6. specify the administrative, operational and technical safeguards and practices it has in place to protect Protected Information that it will receive under this Contract;

12.7. demonstrate that it complies with the requirements of Section 121.3(c) of this Part;

12.8. specify how officers or employees of the Vendor and its assignees who have access to Protected Information receive or will receive training on the federal and state laws governing confidentiality of such data prior to receiving access;

12.9. specify if the Vendor will utilize sub-contractors and how it will manage those relationships and contracts to ensure Protected Information is protected;

12.10. specify how the Vendor will manage data security and privacy incidents that implicate Protected Information including specifying any plans to identify breaches and unauthorized disclosures, and to promptly notify BOCES; and

12.11. describe whether, how and when data will be returned to BOCES, transitioned to a successor contractor, at BOCES's option and direction, deleted or destroyed by the Vendor when the contract is terminated orexpires.

**13. Additional VendorResponsibilities**

Vendor acknowledges that under Education Law Section 2-d and related regulations it has the following obligations with respect to any Protected Information, and any failure to fulfill one of these statutory obligations shall be a breach of this Contract:

13.1 Vendor shall limit internal access to Protected Information to those individuals and Assignees or subcontractors that need access to provide the contracted services;

13.2 Vendor will not use Protected Information for any purpose other than those explicitly authorized in this Contract;

13.3 Vendor will not disclose any Protected Information to any party who is not an authorized representative of the Vendor using the information to carry out Vendor's obligations under this Contract or to the BOCES unless (1) Vendor has the prior written consent of the parent or eligible student to disclose the information to that party, or (ii) the disclosure is required by statute or court order, and notice of the disclosure is provided to BOCES no later than the time of disclosure, unless such notice is expressly prohibited by the statute or court order;

13.4 Vendor will maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of Protected Information in its custody;

13.5 Vendor will use encryption technology to protect data while in motion or in its custody from unauthorized disclosure using a technology or methodology specified by the secretary of the U S. Department of HHS in guidance issued under P.L. 111-5, Section 13402(H)(2);

13.6 Vendor will notify the BOCES of any breach of security resulting in an unauthorized release of student data by the 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 but no more than seven calendar days after the discovery of the breach; and

Where a breach or unauthorized disclosure of Protected Information is attributed to the Vendor, the Vendor shall pay for or promptly reimburse BOCES for the full cost incurred by BOCES to send notifications required by Education Law Section 2-d.

**Signatures**

| **For Wayne-Finger Lakes BOCES/EduTech** | **For (Vendor Name)** |
| --- | --- |
| **Date** 10/12/23 | **Date** 10/11/2023 |

Educational
Technology Service
Genesee Valley
Wayne-Finger Lakes

**Attachment A – Parent Bill of Rights for Data Security and Privacy**

# Wayne-Finger Lakes BOCES (EduTech)

## Parents' Bill of Rights for Data Privacy and Security

The Wayne-Finger Lakes BOCES (EduTech)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 BOCES and school operations.

The Wayne-Finger Lakes BOCES (EduTech)seeks to insure 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 Wayne-Finger Lakes BOCES (EduTech) 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 Board Policy 5500 entitled Family Educational Rights and Privacy Act (FERPA).
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.nysed.gov/data-privacy-security/student-data-inventory 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 the Chief Privacy Officer, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, New York 12234.

Revised October 2019

**Signatures**

| **For Wayne-Finger Lakes BOCES/EduTech** | **For (Vendor Name)** |
|---|---|
| | |
| **Date** 10/12/23 | **Date** 10/11/2023 |

Educational
Technology Service
Genesee Valley
Wayne-Finger Lakes

**Attachment B – Wayne-Finger Lakes BOCES/EduTech Data Privacy and Security Policy**

In accordance with New York State Education Law §2-d, the BOCES hereby implements the requirements of Commissioner's regulations (8 NYCRR §121) and aligns its data security and privacy protocols with the National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 (NIST Cybersecurity Framework or "NIST CSF").

In this regard, every use and disclosure of personally identifiable information (PII) by the BOCES will benefit students and the BOCES (for example, improving academic achievement, empowering parents and students with information, and/or advancing efficient and effective school operations). PII will not be included in public reports or other documents.

The BOCES also complies with the provisions of the Family Educational Rights and Privacy Act of 1974 (FERPA). Consistent with FERPA's requirements, unless otherwise permitted by law or regulation, the BOCES will not release PII contained in student education records unless it has received a written consent (signed and dated) from a parent or eligible student. For more details, see Policy 6320 and any applicable administrative regulations.

In addition to the requirements of FERPA, the Individuals with Disabilities Education Act (IDEA) provides additional privacy protections for students who are receiving special education and related services. For example, pursuant to these rules, the BOCES will inform parents of children with disabilities when information is no longer needed and, except for certain permanent record information, that such information will be destroyed at the request of the parents. The BOCES will comply with all such privacy provisions to protect the confidentiality of PII at collection, storage, disclosure, and destruction stages as set forth in federal regulations 34 CFR 300.610 through 300.627.

The Board of Education values the protection of private information of individuals in accordance with applicable law and regulations. Further, the BOCES Director of Educational Technology is required to notify parents, eligible students, teachers and principals when there has been or is reasonably believed to have been a compromise of the individual's private information in compliance with the Information Security Breach and Notification Act and Board policy and New York State Education Law §2-d

a) "Private information" shall mean **personal information in combination with any one or more of the following data elements, when either the personal information or the data element is not encrypted or encrypted with an encryption key that has also been acquired:

1. Social security number.
2. Driver's license number or non-driver identification card number; or
3. Account number, credit or debit card number, in combination with any required security code, access code, or password, which would permit access to an individual's financial account.
4. Any additional data as it relates to administrator or teacher evaluation (APPR)

"Private information" does not include publicly available information that is lawfully made available to the general public from federal, state or local government records.

**"Personal information" shall mean any information concerning a person, which, because of name, number, symbol, mark or other identifier, can be used to identify that person.

b) Personally Identifiable Information, as applied to student data, means 40 personally identifiable information as defined in section 99.3 of Title 34 of the Code of 41 Federal Regulations implementing the Family Educational Rights and Privacy Act, 20 42 U.S.C 1232-g, and as applied to teacher and principal data, means personally 43 identifying information as such term is defined in Education Law §3012-c(10).

c) Breach means the unauthorized access, use, or disclosure of student data 9 and/or teacher or principal data. Good faith acquisition of personal information by an employee or agent of the BOCES for the purposes of the BOCES is not a breach of the security of the system, provided that private information is not used or subject to unauthorized disclosure.

**Notification Requirements**
**Methods of Notification**

The required notice shall be directly provided to the affected persons and/or their guardians by one of the following methods:

a) Written notice;

b) Secure electronic notice, provided that the person to whom notice is required has expressly consented to receiving the notice in electronic form; and a log of each such notification is kept by the BOCES when notifying affected persons in electronic form. However, in no case shall the BOCES require a person to consent to accepting such notice in electronic form as a condition of establishing any business relationship or engaging in any transaction;

Regardless of the method by which notice is provided, the notice shall include contact information for the notifying BOCES and a description of the categories of information that were, or are reasonably believed to have been, acquired by a person without valid authorization, including specification of which of the elements of personal information and private information were, or are reasonably believed to have been, so acquired. This notice shall take place 60 days of the initial discovery.

In the event that any residents are to be notified, the BOCES shall notify the New York State Chief Privacy Officer, the New York State Cyber Incident Response Team, the office of Homeland Security, and New York State Chief Security Officer as to the timing, content and distribution of the notices and approximate number of affected persons. Such notice shall be made without delaying notice to affected residents.
The Superintendent or his/her designee will establish and communicate procedures for parents, eligible students, and employees to file complaints about breaches or unauthorized releases of student, teacher or principal data (as set forth in 8 NYCRR §121.4). The Superintendent is also authorized to promulgate any and all other regulations necessary and proper to implement this policy.

**Data Protection Officer**

The BOCES has designated a BOCES employee to serve as the BOCES's Data Protection Officer.

The Data Protection Officer is responsible for the implementation and oversight of this policy and any related procedures including those required by Education Law Section 2-d and its implementing regulations, as well as serving as the main point of contact for data privacy and security for the BOCES.

The BOCES will maintain a record of all complaints of breaches or unauthorized releases of student data and their disposition in accordance with applicable data retention policies, including the Records Retention and Disposition Schedule ED-1 (1988; rev. 2004).

**Annual Data Privacy and Security Training**

The BOCES will annually provide data privacy and security awareness training to its officers and staff with access to PII. This training will include, but not be limited to, training on the applicable laws and regulations that protect PII and how staff can comply with these laws and regulations.

**References:**

Education Law §2-d

8 NYCRR §121

Family Educational Rights and Privacy Act of 1974, 20 USC §1232(g), 34 CFR 99

Individuals with Disabilities Education Act (IDEA), 20 USC §1400 et seq., 34 CFR 300.610–300.627


Educational
Technology Service
Genesee Valley
Wayne-Finger Lakes

**Attachment C – Vendor's Data Security and Privacy Plan**

The Wayne-Finger Lakes BOCES Parents Bill of Rights for Data Privacy and Security, which is included as Attachment B to this Addendum, is incorporated into and make a part of this Data Security and Privacy Plan.

(Vendor can attached)

## Addendum B

### PARENTS' BILL OF RIGHTS – SUPPLEMENTAL INFORMATION ADDENDUM

1. **EXCLUSIVE PURPOSES FOR DATA USE**: The exclusive purposes for which "student data" or "teacher or principal data" (as those terms are defined in Education Law Section 2-d and collectively referred to as the "Confidential Data") will be used by CodeHS, Inc. (the "Contractor") are limited to the purposes authorized in the contract between the Contractor and the Wayne-Finger Lakes BOCES/EduTech (the "BOCES") dated 7/1/2023 (the "Contract").

2. **SUBCONTRACTOR OVERSIGHT DETAILS**: The Contractor will ensure that any subcontractors, or other authorized persons or entities to whom the Contractor will disclose the Confidential Data, if any, are contractually required to abide by all applicable data protection and security requirements, including but not limited to those outlined in applicable State and Federal laws and regulations (e.g., the Family Educational Rights and Privacy Act ("FERPA"); Education Law §2-d; 8 NYCRR Part 121).

3. **CONTRACT PRACTICES**: The Contract commences and expires on the dates set forth in the Contract, unless earlier terminated or renewed pursuant to the terms of the Contract. On or before the date the Contract expires, protected data will be exported to the BOCES in csv file **(insert data format)** format and/or destroyed by the Contractor as directed by the BOCES.

4. **DATA ACCURACY/CORRECTION PRACTICES**: A parent or eligible student can challenge the accuracy of any "education record", as that term is defined in FERPA, stored by the BOCES in a Contractor's product and/or service by following the BOCES' procedure for requesting the amendment of education records under FERPA. Teachers and principals may be able to challenge the accuracy of APPR data stored by the BOCES in Contractor's product and/or service by following the appeal procedure in the BOCES' APPR Plan. Unless otherwise required above or by other applicable law, challenges to the accuracy of the Confidential Data shall not be permitted.

5. **SECURITY PRACTICES**: Confidential Data provided to Contractor by the BOCES will be stored in the United States (**insert location**). The measures that Contractor takes to protect Confidential Data will align with the NIST Cybersecurity Framework including, but not necessarily limited to, disk encryption, file encryption, firewalls, and password protection.

6. **ENCRYPTION PRACTICES**: The Contractor will apply encryption to the Confidential Data while in motion and at rest at least to the extent required by Education Law Section 2-d and other applicable law.

Signature: _____

Date: 10/11/2023

CodeHS

New York Ed Law 2-d Compliance

# OVERVIEW

*CodeHS is compliant with NY Ed Law 2-d. Please submit your district's Data Privacy Agreement and Parents' Bill of Rights to hello@codehs.com for review. The following document provides the additional information requested under Ed Law 2-d.*

*In this packet:*

- *Third Party Contractor's Data Security & Privacy Plan*
- *Third Party Contractors Supplemental Agreement*
- *CodeHS Privacy Policy*
- *CodeHS Incident Response Plan*
- *CodeHS Data Deletion Policy*
- *Schedule of Data*

# THIRD-PARTY CONTRACTOR'S DATA SECURITY AND PRIVACY PLAN

## *Exclusive Purposes for Data Use*

*CodeHS will only use student data for the purposes outlined in this agreement and the CodeHS Terms of Use and Privacy Policy.*

## *Data Accuracy/Correction Practices*

*Parents or students should contact their LEA directly with requests to challenge the accuracy of their data stored on CodeHS.*

*LEA privacy representatives should contact CodeHS at hello@codehs.com with any requests to correct data.*

## *Subcontractor Oversight Details*

*CodeHS does not utilize subcontractors. Any subcontractors CodeHS uses in the future will be required to uphold privacy policies and procedures that are of an equal or greater standard than the terms of this agreement.*

*Current list of any subcontractors can be found at https://codehs.com/subcontractors.*

## *Security Practices*

*Data is stored with Amazon Web Services ("AWS") in encrypted databases. All data and traffic are encrypted using HTTPS.*

# THIRD-PARTY CONTRACTOR'S DATA SECURITY AND PRIVACY SUPPLEMENTAL AGREEMENT

In accordance with its obligations under the District's Parents' Bill Rights and Data Privacy and Security Agreement, the Contractor represents and warrants that its data security and privacy plan described below or attached hereto contains the following minimum required provisions:

(i) Contractor will implement State and federal data security and privacy contract requirements for the duration of its contract that is consistent with the school district's data security and privacy policy by:

*CodeHS Privacy Policy and Terms of use can be found at https://codehs.com/privacy and https://codehs.com/terms, respectively. All employees with access to data are trained to uphold these documented privacy standards and procedures, and all data is encrypted using HTTPS.*

(ii) Contractor will use the following administrative, operational and technical safeguards to protect personally identifiable information:

*All data and traffic are encrypted using HTTPS. Data is stored with AWS in encrypted databases.*

(iii) Contractor has complied with requirements of §121.3(c) of the Commissioner's Regulations by providing and complying with the supplemental contractor information attached to its contract or written agreement with the District, or as follows:

*CodeHS supplemental Data Security and Privacy Plan can be found above, on the first page of https://codehs.com/privacy/newyork.*

(iv) Contractor's employees and any assignees with access to student data, or teacher or principal data have received or will receive training on relevant confidentiality laws, before receiving access to such data, as follows:

*All employees receive annual Cybersecurity training. All employees with access to PII receive training on confidentiality laws and company procedures to ensure that PII is kept secure and confidential.*

(v) Contractor will use the following subcontractors and will ensure that personally identifiable information received by its subcontractors is protected, as follows:

*CodeHS does not utilize subcontractors. Any subcontractors CodeHS uses in the future will be required to uphold privacy policies and procedures that are of an equal or greater standard than the terms of this agreement.*

*Current list of any subcontractors can be found at https://codehs.com/subcontractors.*

(vi) Contractor will implement an action plan for handling any breach or unauthorized disclosure of personally identifiable information and will promptly notify the school district of any breach or unauthorized disclosure as follows:

*CodeHS Incident Response Plan can be found below and is also available at https://codehs.com/incident_response.*

(vii) Data will be returned, transitioned to a successor contractor, deleted or destroyed when the contract ends or is terminated as follows:

*Upon written request by the district, CodeHS will delete all student data.*

*CodeHS Data Deletion Policy can be found below and is also available at https://codehs.com/data_deletion.*

# CODEHS PRIVACY POLICY

## *About CodeHS*

CodeHS, Inc. is a comprehensive online coding platform to help schools and districts teach computer science. The platform includes web-based curriculum, teacher tools and resources, and professional development.

Please read this Privacy Policy carefully before accessing or using the Website. In this Policy, we refer to these products as the "Website" or the "Services".

## *What is this policy all about?*

This privacy policy (the "Policy") explains what data we collect, why we collect it, and what we do with it. It applies to you if you're a student, a teacher, or anyone else who uses our Website.

This Policy applies to information that we collect when you use our Services online. It does not apply to information we may collect offline or if you provide any information to a third party (including through any application or content that may link to or be accessible from the Website). We use the term "Personal Information" to refer to any information that would identify you as an individual (e.g. your name and/or email address).

By using the Service, you accept and agree to this Privacy Policy. Your use of the Service is also governed by the Terms of Use. You should read both of these documents together.

## *What information do we collect and why?*

We aim to collect only the information necessary to provide you with a great learning or teaching experience. We receive and store any information you knowingly enter on the Services. We also receive and store some information automatically. The following section provides further explanation of what we collect and why.

**Account information**
When you create an account (as either a student or a teacher), you need to enter your name, a username, and your email address. For students in schools, you will enter a class code provided by your teacher to link your account to your classroom and your school. For teachers, you will be asked to provide information about your school so we can verify that you are a real teacher.

**Technical data**

As you use our Website, we may use automatic data collection technologies to collect information about your equipment, browsing actions, and patterns. For example, we may collect: details of your visits to our Website, including traffic data, location data, logs, and other communication data; and information about your computer and internet connection, including your IP address, operating system, and browser type.

The information we collect automatically is statistical data and does not include Personal Information. It helps us to improve our Website and to deliver a better and more personalized service, including by enabling us to:

- estimate our audience size and usage patterns;
- monitor site performance and uptime;
- resolving technical issue for Website users;
- store information about your preferences, allowing us to customize our Website for you; and
- recognize you when you return to our Website.

The technologies we use for this automatic data collection may include tools such as cookies and web beacons. Cookies are small files that websites place on your computer as you browse the web. Web beacons (also referred to as clear gifs, pixel tags, and single-pixel gifs) are small electronic files that permit us, for example, to count users who have visited certain pages or opened an email and for other related website statistics (for example, recording the popularity of certain website content and verifying system and server integrity). You may choose to disable cookies in your browser settings. However, if you choose to do this, many of our Website's features may not function properly.

**Coursework and grading**
If you are a student, we collect information about your projects, including the responses you provide, how many attempts you made, and the time taken. This helps us to give you a great experience with our Service, including allowing you to save your work, helping us to improve our courses, and allowing teachers to assess and monitor students' progress.

**Student code, programs, projects, and uploaded files**
If you are logged in to your CodeHS account, we save the code and programs you have written. We do this so that teachers and students can revisit their work at a later time, and can continue working on their programs where they left off. As a student or a teacher, you can also upload content through the Website. If a student or teacher uploads content as part of writing a program, that content will be stored on the Website.

**Student and teacher websites**
As you work on CodeHS, students and teachers have the option to create personal websites. You can upload and create content on these sites, which will then become publicly available.

**Messages**
Students may send messages to their teacher through the Website, and a teacher may send messages to their students. In the case where an individual learner or school has specifically signed up for tutoring services, messages may be sent between students, teachers, and tutors. Only the participants in each of these conversations may see the contents of the messages.

**Surveys and demographics**
Occasionally we will send out optional online surveys to students asking for data such as age, gender, race and academic background. This data is only ever used in the aggregate and for the purposes of improving the Website and ensuring that we are reaching a diverse and representative group of learners.

## *Who can access your information?*

We do not sell or rent your Personal Information to any third party for any purpose, including advertising or marketing. We do not allow any advertising on our services.

We restrict access to your information to CodeHS employees, contractors and agents who need to know that information in order to process it for us and who are subject to strict contractual security standards and confidentiality obligations. They may be disciplined or their contract terminated if they fail to meet these obligations.

Account information, coursework and grading, as well as student programs, projects, and uploaded files can be accessed by the student who created them and his or her teacher. Messages are accessible to participants in that conversation. All users of the Website must abide by the Terms of Use, which include obligations about interacting with other users.

We may disclose information that we collect or you provide as described in this privacy policy to a buyer or other successor in the event of a merger, divestiture, restructuring, reorganization, dissolution, or other sale or transfer of some or all of our assets, in which Personal Information that we hold is among the assets transferred. This Privacy Policy will continue to apply to your information, and any acquirer would only be able to handle your Personal Information as per this Policy (unless you give consent to a new policy). We will provide you with prompt notice of an acquisition, by posting on our homepage, or by email to your email address that you provided to us. If you do not consent to the use of your Personal Information by such a successor company, you may request that the company delete it.

We may also disclose your Personal Information:

- to comply with any court order, law, or legal process, including to respond to any government or regulatory request;
- to ensure site security, or to enforce or apply our Terms of Use and other agreements, including for billing and collection purposes;
- if we believe disclosure is necessary or appropriate to protect the rights, property, or safety of CodeHS, Inc., our customers, or others; and
- to a state or local educational agency, including schools and school districts, for K-12school purposes, as permitted by state or federal law.

We may disclose aggregated information about our users, and information that does not identify any individual, without restriction.

## *How do we store and delete your information?*

Website users may update, correct, or remove Personal Information in their CodeHS accounts at any time via the Account Settings page.

Students and teachers may deactivate their account at any time from the Account Settings page.

A teacher or a student may request deletion of your own Personal Information by sending us an email at hello@codehs.com. In appropriate circumstances, teachers and parents may also request deletion of a student's Personal Information. IN SUCH CASE, WE WILL NO LONGER ALLOW THE APPLICABLE USER TO USE THE SERVICES. We will delete your or your student's information using reasonable measures to protect against unauthorized access to, or use of, the information in connection with its deletion. When we delete a user's Personal Information, it will be deleted from our active databases but we may retain an archived copy of such user's records as required by law or for legitimate business purposes.

We will retain Personal Information, including after the school term in which a teacher or student uses the Services, for only as long as is reasonably necessary to fulfill the purpose for which the information was collected. Generally, CodeHS will delete a user's Personal Information 4 years after the user's last login to the Services.

## *How do we protect and secure your information?*

We have implemented reasonable measures designed to secure your information from accidental loss and from unauthorized access, use, alteration, and disclosure. Any payment information is transmitted using HTTPS encryption and is processed through Stripe, a third party payment provider. CodeHS does not directly collect or store payment instruments.

The safety and security of your information also depends on you. You are responsible for choosing a strong password and keeping it confidential.

If there is a data breach affecting your information, we will comply with any relevant legal or regulatory notification requirements.

## *Children under the age of 13*

Because some of our users may be interested in it, we have included some information below related to the Children's Online Privacy and Protection Act ("COPPA"). COPPA requires that online service providers obtain parental consent before they knowingly collect personally identifiable information online from children who are under 13. Therefore, we only collect Personal Information through the Services from a child under 13 where that student's school, district, and/or teacher has agreed (via the terms described in the Terms of Use) to obtain parental consent for that child to use the Services and disclose Personal Information to us. A parent or guardian may sign up his or her child for the Services and provide Personal Information about that child to us. However, no child under 13 may send us any Personal Information unless he or she has signed up through his or her school, district or teacher and such school, district or teacher has obtained parental consent for that child to use the Services and disclose Personal Information to us. If you are a student under 13, please do not send any Personal Information to us if your school, district, and/or teacher has not obtained this prior consent from your parent or guardian, and please do not send any Personal Information other than what we request from you in connection with the Services. If we learn we have collected Personal Information from a student under 13 without parental consent from his or her parent or guardian or obtained by his or her school, district, and/or teacher, or if we learn a student under 13 has provided us personal information beyond what we request from him or her, we will delete that information as quickly as possible. If you believe that a student under 13 may have provided us personal information in violation of this paragraph, please contact us at hello@codehs.com.

If you are signing up for this service and creating accounts on behalf of student(s), you represent and warrant that you are either (a) a teacher or school administrator or otherwise authorized by a school or district to sign up on behalf of students or (b) the parent of such student(s). If you are a school, district, or teacher, you represent and warrant that you are solely responsible for complying with COPPA, meaning that you must obtain advance written consent from all parents or guardians whose children under 13 will be accessing the Services. When obtaining consent, you must provide parents and guardians with these Terms and our Privacy Policy. You must keep all consents on file and provide them to us if we request them. If you are a teacher, you represent and warrant that you have permission and authorization from your school and/or district to use the Services as part of your curriculum, and for purposes of COPPA compliance, you represent and warrant that you are entering into these Terms on behalf of your school and/or district.

## *Changes to the Privacy Policy*

Our Privacy Policy may change from time to time. We will post any changes we make on this page with a notice on the Website's homepage that the privacy policy has been updated. If we make material changes to this Privacy Policy, we will email you at the email address associated with your account. You can access older versions of this Privacy Policy at codehs.com/privacy2013.

## *Questions?*

To ask questions or comment on this Privacy Policy and our privacy practices, contact us at hello@codehs.com.

# INCIDENT RESPONSE PLAN

*This document describes the procedures CodeHS will follow in response to the report of a data breach or security incident.*

## Discovery and Response to Incident

1. If the person discovering the incident is a member of the IT department or affected department, they will proceed to step 5.
2. If the person discovering the incident is not a member of the IT department or affected department, they will call the CodeHS Headquarters at 415-889-3376.
3. The headquarters office manager will refer to the IT emergency contact list or affected department contact list and call the designated numbers in order on the list. The grounds security office will log:
    a. The name of the caller
    b. Time of the call
    c. Contact information about the caller
    d. The nature of the incident
    e. What equipment or persons were involved?
    f. Location of equipment or persons involved
    g. How the incident was detected
    h. When the event was first noticed that supported the idea that the incident occurred.
4. The IT staff member or affected department staff member who receives the call (or discovered the incident) will refer to their contact list for both management personnel to be contacted and incident response members to be contacted. The staff member will call those designated on the list. The staff member will contact the incident response manager using both email and phone messages while being sure other appropriate and backup personnel and designated managers are contacted. The staff member will log the information received in the same format as the grounds security office in the previous step. The staff member could possibly add the following:
    a. Is the equipment affected business-critical?
    b. What is the severity of the potential impact?
    c. Name of system being targeted, along with operating system (if applicable), IP address, and location.
    d. IP address and any information about the origin of the attack.
5. Contacted members of the response team will meet or discuss the situation over the telephone and determine a response strategy.
    a. Is the incident real or perceived?
    b. Is the incident still in progress?
    c. What data or property is threatened and how critical is it?
    d. What is the impact on the business should the attack succeed? Minimal, serious, or critical?
    e. What system or systems are targeted, where are they located physically and on the network?
    f. Is the incident inside the trusted network?
    g. Is the response urgent?
    h. Can the incident be quickly contained?
    i. Will the response alert the attacker and do we care?
    j. What type of incident is this? Example: virus, worm, intrusion, abuse, damage.

6. An incident ticket will be created. The incident will be categorized into the highest applicable level of one of the following categories:
    a. Category one - A threat to sensitive data
    b. Category two - A threat to computer systems
    c. Category three - A disruption of services
7. Team members will establish and follow one of the following procedures basing their response on the incident assessment:
    a. Worm response procedure
    b. Virus response procedure
    c. System failure procedure
    d. Active intrusion response procedure - Is critical data at risk?
    e. Inactive Intrusion response procedure
    f. System abuse procedure
    g. Property theft response procedure
    h. Website denial of service response procedure
    i. Database or file denial of service response procedure
    j. Spyware response procedure.

    The team may create additional procedures which are not foreseen in this document. If there is no applicable procedure in place, the team must document what was done and later establish a procedure for the incident.
8. Team members will use forensic techniques, including reviewing system logs, looking for gaps in logs, reviewing intrusion detection logs, and interviewing witnesses and the incident victim to determine how the incident was caused.
9. Team members will recommend changes to prevent the occurrence from happening again or infecting other systems.
10. Upon management approval, the changes will be implemented.
11. Team members will restore the affected system(s) to the uninfected state. They may do any or more of the following:
    a. Re-install the affected system(s) from scratch and restore data from backups if necessary. Preserve evidence before doing this.
    b. Make users change passwords if passwords may have been sniffed.
    c. Be sure the system has been hardened by turning off or uninstalling unused services.
    d. Be sure the system is fully patched.
    e. Be sure real-time virus protection and intrusion detection are running.
    f. Be sure the system is logging the correct events and to the proper level.
12. Documentation—the following shall be documented:
    a. How the incident was discovered
    b. The category of the incident
    c. How the incident occurred, whether through email, firewall, etc.
    d. Where the attack came from, such as IP addresses and other related information about the attacker
    e. What the response plan was
    f. What was done in response?
    g. Whether the response was effective

13. Evidence Preservation—make copies of logs, email, and other communication. Keep lists of witnesses. Keep evidence as long as necessary to complete prosecution and beyond in case of an appeal.
14. Notify proper external agencies—team members will notify the police and other appropriate agencies if prosecution of the intruder is possible.
15. Review response and update policies—team members will plan and take preventative steps so the intrusion can't happen again. The following factors will be considered:
    a. Whether an additional policy could have prevented the intrusion
    b. Whether a procedure or policy was not followed which allowed the intrusion, and then consider what could be changed to ensure that the procedure or policy is followed in the future
    c. Was the incident response appropriate? How could it be improved?
    d. Was every appropriate party informed in a timely manner?
    e. Were the incident-response procedures detailed and did they cover the entire situation? How can they be improved?
    f. Have changes been made to prevent a re-infection? Have all systems been patched, systems locked down, passwords changed, anti-virus updated, email policies set, etc.?
    g. Have changes been made to prevent a new and similar infection?
    h. Should any security policies be updated?
    i. What lessons have been learned from this experience?

## Notification to LEA

In the event that Student Data is accessed or obtained by an unauthorized individual, CodeHS shall provide notification to LEA within forty-eight (48) hours of discovering the breach.

1. CodeHS shall follow the process described below:
    a. The security breach notification shall be written in plain language, shall be titled "Notice of Data Breach," and shall present the information described herein under the following headings: "What Happened," "What Information Was Involved," "What We Are Doing," "What You Can Do," and "For More Information." Additional information may be provided as a supplement to the notice.
    b. The security breach notification described above in section (a) shall include, at a minimum, the following information:
        i. The name and contact information of the reporting LEA subject to the data breach.
        ii. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.
        iii. If the information is possible to determine at the time the notice is provided, then either (1) the date of the breach, (2) the estimated date of the breach, or (3) the date range within which the breach occurred. The notification shall also include the date of the notice.
        iv. Whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided.
        v. A general description of the breach incident, if that information is possible to determine at the time the notice is provided.
    c. At LEA's discretion, the security breach notification may also include any of the following:
        i. Information about what the agency has done to protect individuals whose information has been breached.

ii. Advice on steps that the person whose information has been breached may take to protect himself or herself.

d. CodeHS agrees to adhere to all requirements in federal law with respect to a data breach related to the Student Data, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation of any such data breach.
e. At the request and with the assistance of the District, CodeHS shall notify the affected parent, legal guardian or eligible pupil of the unauthorized access, which shall include the information listed in subsections (b) and (c), above.
f. In the event of a breach originating from LEA's use of the Services, CodeHS shall cooperate with LEA to the extent necessary to expeditiously secure Student Data.

# DATA DELETION POLICY

*This document describes the procedures CodeHS will follow regarding data deletion.*

If a separate data privacy agreement is executed between CodeHS and a customer school or district, that agreement will take precedence over this policy.

## End of Life Data Deletion

Upon written request from the LEA, CodeHS will dispose of or provide a mechanism for the LEA to transfer Student Data obtained under the Service Agreement, within sixty (60) days of the date of said request and according to a schedule and procedure as the Parties may reasonably agree. The duty to dispose of Student Data shall not extend to Student Data that had been De-Identified or placed in a separate student account.

CodeHS

# SCHEDULE OF DATA

| Category of Data | Elements | Check if used by your system |
|---|---|---|
| Application Technology Meta Data | IP Addresses, Use of cookies etc. | X |
| | Other application technology meta data (specify): | X (Browser, OS used) |
| | | |
| Application Use Statistics | Meta data on user interaction with application | X |
| | | |
| Assessment | Standardized test scores | |
| | Observation data | |
| | Other assessment data (specify): Student Personality Assessments | |
| | | |
| Attendance | Student school (daily) attendance data | |
| | Student class attendance data | X |
| | | |
| Communications | Online communications that are captured (emails, blog entries) | X |
| | | |
| Conduct | Conduct or behavioral data | |
| | | |
| Demographics | Date of Birth | |
| | Place of Birth | |
| | Gender | |
| | Ethnicity or race | |
| | Language information (native, preferred or primary language spoken by student) | |
| | Other demographic information (specify): | |
| Enrollment | Student school enrollment | |
| | Student grade level | |
| | Homeroom | |
| | Guidance counselor | |
| | Specific curriculum programs | |
| | Year of graduation | |
| | Other enrollment information (specify): | |

| Category of Data | Elements | Check if used by your system |
|---|---|---|
| Parent/ Guardian Name | First and/or Last | |
| | | |
| Schedule | Student scheduled courses | |
| | Teacher names | |
| | | |
| Special Indicator | English language learner information | |
| | Low income status | |
| | Medical alerts | |
| | Student disability information | |
| | Specialized education services (IEP or 504) | |
| | Living situations (homeless/foster care) | |
| | Other indicator information(specify): First Generation College Student | |
| | | |
| Student Contact Information | Address | |
| | Email | X |
| | Phone | |
| | | |
| Student Identifiers | Local (School district) ID number | |
| | State ID number | |
| | Vendor/App assigned student ID number | X |
| | Student app username | X |
| | Student app passwords | X |
| | | |
| Student Name | First and/or Last | X |
| | | |
| Student In-App Performance | Program/application performance (typing program-student types 60 wpm, reading program-student reads below grade level) | X |
| | | |
| Student Program Membership | Academic or extracurricular activities a student may belong to or participate in | |

| Category of Data | Elements | Check if used by your system |
|---|---|---|
| Student Survey Responses | Student responses to surveys or questionnaires | X |
| | | |
| Student work | Student generated content, writing, pictures etc. | X |
| | Other student work data (Please specify): | |
| | | |
| Transcript | Student course grades | |
| | Student course data | X |
| | Student course grades/performance scores | |
| | Other transcript data (Please specify): | |

| Category of Data | Elements | Check if used by your system |
|---|---|---|
| Transportation | Student bus assignment | |
| | Student pick up and/or drop off location | |
| | Student bus card ID number | |
| | Other transportation data (Please specify): | |
| | | |
| Other | Please list each additional data element used, stored or collected by your application | |

CodeHS

# NIST CSF TABLE

| 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. | 4 - CodeHS keeps an inventory of devices used by employees and personal devices cannot be used without manager approval. Personally identifiable information of CodeHS students is never stored on employee devices. CodeHS does not utilize subcontractors but does utilize Amazon Web Services and Google as 3rd party systems to achieve business purposes. |
| | **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. | 6 - The CodeHS company mission and values are communicated biweekly in each all staff meeting, the organization's quarterly and annual objectives are communicated in each all staff meeting, and staff responsibilities and stakeholders are managed by each team. CodeHS staff are trained on their responsibilities for protecting school data during onboarding and are required to sign our CodeHS Employee Student Data Confidentiality Agreement as a condition of employment. |
| | **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. | 4 - CodeHS has documented and defined processes for student data confidentiality, data deletion, incident response, and internal documentation for federal, state-specific, and district-specific regulatory requirements that CodeHS employees must abide by |
| | **Risk Assessment (ID.RA):** The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals. | 4 - CodeHS maintains an internal list of cybersecurity risks to the CodeHS service, infrastructure, and reputation, as well as steps that have been taken to mitigate risks. This document is continually updated and is used in employee onboarding and training. |
| | **Risk Management Strategy (ID.RM):** The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions. | 4 - CodeHS Leadership monitors the organization's risks and regularly meets to discuss and document our risk 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. | 7 - The services provided by CodeHS do not depend on a traditional supply chain. The physical servers and databases the CodeHS service depends on are spread across multiple availability zones to ensure redundancy and availability, managed by Amazon Web Services, and CodeHS guarantees 99.9% uptime for its users http://status.codehs.com/ |
| 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. | 5 - Physical access to CodeHS web servers and databases is secured and managed by Amazon Web Services. Remote access is managed by AWS role based authentication to restrict access to only trained and authorized employees. CodeHS enforces 2 Factor Authentication for employee accounts across all web services. User identities are permissioned and bound to transactions within the CodeHS service. |
| | **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. | 4 - CodeHS employees receive general cybersecurity training during onboarding as well as annual training for current employees. Role-based training is provided based on each employee's role and responsibilities. The CodeHS service itself teaches the fundamentals of cybersecurity and employees are additionally required to complete the curriculum we provide to our users. |
| | **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. | 5 - All CodeHS data at rest is encrypted and protected by AWS. All database instances, logs, backups, and snapshots are encrypted using the industry standard AES-256 encryption algorithm. All CodeHS data in transit is encrypted over HTTPS. CodeHS development and testing environments are separate from the production environment. CodeHS uses AWS autoscaling and load balancing to ensure adequate capacity is maintained to keep CodeHS services available as traffic fluctuates. |
| | **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. | 5 - CodeHS has a hardened baseline configuration rolled out across devices and critical assets as well as a documented, tested, and iteratively improved process for rolling out updates. CodeHS creates daily encrypted database backups in AWS and keeps them available for 30 days. CodeHS has a documented process for destroying user data by request as needed for privacy compliance. New staff are trained in cybersecurity policies and practices as part of onboarding as well as annually for current employees. CodeHS has a documented and tested Incident Response Plan: https://codehs.com/incidentresponseplan |

| | | |
|---|---|---|
| | **Maintenance (PR.MA):** Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures. | 5 - Maintenance of the physical CodeHS system components is managed by AWS. CodeHS has a documented, tested, and iteratively improved process for rolling out maintenance updates to the CodeHS service itself that allows CodeHS to test and document changes before they are applied to the production environment, and have zero downtime for users. Maintenance that may result in downtime is rare, scheduled, and communicated ahead of time both on the CodeHS website as well as on http://status.codehs.com/ where anyone can subscribe to notifications. |
| | **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. | 5 - CodeHS utilizes AWS security solutions including Amazon Web Application Firewall and Amazon CloudFront to log, detect, and block malicious web traffic including DDoS attacks. CodeHS uses AWS autoscaling and load balancing to ensure adequate capacity is maintained in normal and adverse conditions to keep CodeHS services available at all times. |
| **DETECT (DE)** | **Anomalies and Events (DE.AE):** Anomalous activity is detected and the potential impact of events is understood. | 5 - CodeHS uses Amazon Web Application Firewall and Amazon CloudFront to log, detect, and block malicious web traffic including DDoS attacks. Incident alert thresholds are established and updated to notify CodeHS of anomalous events. |
| | **Security Continuous Monitoring (DE.CM):** The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures. | 4 - The physical environment that provides the CodeHS service is managed by AWS. AWS resources are remotely monitored and alerts are configured to identify cybersecurity events and verify the effectiveness of protective measures. CodeHS utilizes AWS Virtual Private Cloud to monitor connections to critical assets and ensure no unauthorized connections are possible. |
| | **Detection Processes (DE.DP):** Detection processes and procedures are maintained and tested to ensure awareness of anomalous events. | 5 - Personnel roles and responsibilities for detection are established and understood to ensure accountability. AWS CloudWatch and Web Application Firewall rules are maintained, tested, and continuously improved to ensure awareness of anomalous events. Event detection is communicated both in well defined internal channels as well as externally via status.codehs.com |
| **RESPOND (RS)** | **Response Planning (RS.RP):** Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents. | 5 - CodeHS has a documented and maintained incident response plan that is executed by personnel during a cybersecurity incident |
| | **Communications (RS.CO):** Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies). | 4 - CodeHS personnel know their roles and responsibilities and information is shared both internally and with external stakeholders in accordance with the CodeHS incident response plan |

| | | |
|---|---|---|
| | **Analysis (RS.AN):** Analysis is conducted to ensure effective response and support recovery activities. | 5 - Personnel use forensic techniques, including reviewing system logs, looking for gaps in logs, reviewing intrusion detection logs, and interviewing witnesses and the incident victim to determine how the incident was caused. The impact of the incident is determined and the incident is categorized in accordance with the CodeHS incident response plan |
| | **Mitigation (RS.MI):** Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident. | 5 - Immediate action is taken to contain the impact of any incident and personnel will recommend changes to prevent the occurrence from happening again or infecting other systems. Upon management approval, the changes will be implemented and documented. |
| | **Improvements (RS.IM):** Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities. | 5 - A post mortem is conducted after any incident to incorporate lessons learned, document what happened and what was done, and communicate changes made to prevent incidents in the future. |
| 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. | 5 - CodeHS has a recovery plan that is continuously maintained and executed after an incident. CodeHS personnel restore the affected system(s) to their uninfected state after an incident. |
| | **Improvements (RC.IM):** Recovery planning and processes are improved by incorporating lessons learned into future activities. | 5 - The CodeHS recovery plan is updated after a post mortem to incorporate lessons learned and update technologies, strategies, and processes going forward |
| | **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). | 5 - CodeHS is well aware of the effects cybersecurity incidents can have on the CodeHS reputation and has a plan in place to maintain public relations and communicate recovery activities both internally and externally according to our incident response plan. |