

# DATA PRIVACY AGREEMENT

## **Guilderland Central School District and Desmos**

This Data Privacy Agreement ("DPA") is by and between the Guilderland Central School District ("EA"), an Educational Agency, and Desmos Studio PBC ("Contractor"), collectively, the "Parties".

### ARTICLE I: DEFINITIONS

As used in this DPA, the following terms shall have the following meanings:

1. **Breach:** The unauthorized acquisition, access, use, or disclosure of Personally Identifiable Information in a manner not permitted by State and federal laws, rules and regulations, or in a manner which compromises its security or privacy, or by or to a person not authorized to acquire, access, use, or receive it, or a Breach of Contractor's security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personally Identifiable Information.
2. **Commercial or Marketing Purpose:** means the sale, use or disclosure of Personally Identifiable Information for purposes of receiving remuneration, whether directly or indirectly; the sale, use or disclosure of Personally Identifiable Information for advertising purposes; or the sale, use or disclosure of Personally Identifiable Information to develop, improve or market products or services to students.
3. **Disclose:** To permit access to, or the release, transfer, or other communication of personally identifiable information by any means, including oral, written or electronic, whether intended or unintended.
4. **Education Record:** An education record as defined in the Family Educational Rights and Privacy Act and its implementing regulations, 20 U.S.C. 1232g and 34 C.F.R. Part 99, respectively.
5. **Educational Agency:** As defined in Education Law 2-d, a school district, board of cooperative educational services, school, charter school, or the New York State Education Department.
6. **Eligible Student:** A student who is eighteen years of age or older.
7. **Encrypt or Encryption:** As defined in the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule at 45 CFR 164.304, means the use of an algorithmic process to transform Personally Identifiable Information into an unusable, unreadable, or indecipherable form in which there is a low probability of assigning meaning without use of a confidential process or key.
8. **NIST Cybersecurity Framework:** The U.S. Department of Commerce National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity Version 1.1.

9. **Parent:** A parent, legal guardian or person in parental relation to the Student.
10. **Personally Identifiable Information (PII):** Means personally identifiable information as defined in section 99.3 of Title 34 of the Code of Federal Regulations implementing the Family Educational Rights and Privacy Act, 20 U.S.C 1232g , and Teacher or Principal APPR Data, as defined below.
11. **Release:** Shall have the same meaning as Disclose.
12. **School:** Any public elementary or secondary school including a charter school, universal pre-kindergarten program authorized pursuant to Education Law § 3602-e, an approved provider of preschool special education, any other publicly funded pre-kindergarten program, a school serving children in a special act school district as defined in Education Law § 4001, an approved private school for the education of students with disabilities, a State-supported school subject to the provisions of Article 85 of the Education Law, or a State-operated school subject to the provisions of Articles 87 or 88 of the Education Law.
13. **Student:** Any person attending or seeking to enroll in an Educational Agency.
14. **Student Data:** Personally identifiable information as defined in section 99.3 of Title 34 of the Code of Federal Regulations implementing the Family Educational Rights and Privacy Act, 20 U.S.C 1232g.
15. **Subcontractor:** Contractor's non-employee agents, consultants and/or subcontractors engaged in the provision of services pursuant to the Service Agreement.
16. **Teacher or Principal APPR Data:** Personally Identifiable Information from the records of an Educational Agency relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of Education Law §§ 3012-c and 3012-d.

## ARTICLE II: PRIVACY AND SECURITY OF PII

### 1. Compliance with Law.

In order for Contractor to provide certain services ("Services") to the EA pursuant to a contract dated 5/16/23 ("Service Agreement"); Contractor may receive PII regulated by several New York and federal laws and regulations, among them, the Family Educational Rights and Privacy Act ("FERPA") at 12 U.S.C. 1232g (34 CFR Part 99); Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. 6501-6502 (16 CFR Part 312); Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h (34 CFR Part 98); the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. 1400 et seq. (34 CFR Part 300); New York Education Law Section 2-d; and the Commissioner of Education's Regulations at 8 NYCRR Part 121. The Parties enter this DPA to address the requirements of New York law. Contractor agrees to maintain the confidentiality and security of PII in accordance with applicable New York, federal and local laws, rules and regulations.

### 2. Authorized Use.

Contractor has no property or licensing rights or claims of ownership to PII, and Contractor must not use PII for any purpose other than to provide the Services set forth in the Service Agreement. Neither the Services provided nor the manner in which such Services are provided shall violate New York law.

**3. Data Security and Privacy Plan.**

Contractor shall adopt and maintain administrative, technical and physical safeguards, measures and controls to manage privacy and security risks and protect PII in a manner that complies with New York State, federal and local laws and regulations and the EA's policies. Education Law Section 2-d requires that Contractor provide the EA with a Data Privacy and Security Plan that outlines such safeguards, measures and controls including how the Contractor will implement all applicable state, federal and local data security and privacy requirements. Contractor's Data Security and Privacy Plan is attached to this DPA as Exhibit C.

**4. EA's Data Security and Privacy Policy**

State law and regulation requires the EA to adopt a data security and privacy policy that complies with Part 121 of the Regulations of the Commissioner of Education and aligns with the NIST Cyber Security Framework. Contractor shall comply with the EA's data security and privacy policy and other applicable policies.

**5. Right of Review and Audit.**

Upon request by the EA, Contractor shall provide the EA with copies of its policies and related procedures that pertain to the protection of PII. It may be made available in a form that does not violate Contractor's own information security policies, confidentiality obligations, and applicable laws. In addition, not more than once annually, Contractor may be required to undergo an audit of its privacy and security safeguards, measures and controls as it pertains to alignment with the requirements of New York State laws and regulations, the EA's policies applicable to Contractor, and alignment with the NIST Cybersecurity Framework performed by an independent third party, and provide the audit report to the EA. Contractor may provide the EA with a recent industry standard independent audit report on Contractor's privacy and security practices as an alternative to undergoing an audit.

**6. Contractor's Employees and Subcontractors.**

- (a) Contractor shall only disclose PII to Contractor's employees and subcontractors who need to know the PII in order to provide the Services and the disclosure of PII shall be limited to the extent necessary to provide such Services. Contractor shall ensure that all such employees and subcontractors comply with the terms of this DPA.
- (b) Contractor must ensure that each subcontractor performing functions pursuant to the Service Agreement where the subcontractor will receive or have access to PII is contractually bound by a written agreement that includes confidentiality and data

security obligations equivalent to, consistent with, and no less protective than, those found in this DPA.

- (c) Contractor shall examine the data security and privacy measures of its subcontractors prior to utilizing the subcontractor. If at any point a subcontractor fails to materially comply with the requirements of this DPA, Contractor shall: notify the EA and remove such subcontractor's access to PII; and, as applicable, retrieve all PII received or stored by such subcontractor and/or ensure that PII has been securely deleted and destroyed in accordance with this DPA. In the event there is an incident in which the subcontractor compromises PII, Contractor shall follow the Data Breach reporting requirements set forth herein.
- (d) Contractor shall take full responsibility for the acts and omissions of its employees and subcontractors.
- (e) Contractor must not disclose PII to any other party unless:
  - (i) The Contractor has received written permission from a parent or eligible student to whom the data pertains to beforehand; or
  - (ii) Such disclosure is required by statute, court order or subpoena, and the Contractor makes a reasonable effort to notify the EA of the court order or subpoena in advance of compliance but in any case, provides notice to the EA no later than the time the PII is disclosed, unless such disclosure to the EA is expressly prohibited by the statute, court order or subpoena.

## **7. Training.**

Contractor shall ensure that all its employees and Subcontractors who have access to PII have received or will receive training on the federal and state laws governing confidentiality of such data prior to receiving access.

## **8. Termination**

The obligations of this DPA shall continue and shall not terminate for as long as the Contractor or its sub-contractors retain PII or retain access to PII.

## **9. Data Return and Destruction of Data.**

- (a) Protecting PII from unauthorized access and disclosure is of the utmost importance to the EA, and Contractor agrees that it is prohibited from retaining PII or continued access to PII or any copy, summary or extract of PII, on any storage medium (including, without limitation, in secure data centers and/or cloud-based facilities) whatsoever beyond the period of providing Services to the EA, unless such retention is either expressly authorized for a prescribed period by the Service Agreement or other written agreement between the Parties, or expressly requested by the EA for purposes of facilitating the transfer of PII to the EA or expressly required by law. As applicable, upon expiration or termination of the Service

Agreement, and receipt of a written request, Contractor shall transfer PII, in a format agreed to by the Parties to the EA.

- (b) If applicable, once the transfer of PII has been accomplished in accordance with the EA's written election to do so, Contractor agrees to return or destroy all PII when the purpose that necessitated its receipt by Contractor has been completed. Thereafter, with regard to all PII (including without limitation, all hard copies, archived copies, electronic versions, electronic imaging of hard copies) as well as any and all PII maintained on behalf of Contractor in a secure data center and/or cloud-based facilities that remain in the possession of Contractor or its Subcontractors, Contractor shall ensure that PII is securely deleted and/or destroyed in a manner that does not allow it to be retrieved or retrievable, read or reconstructed. Hard copy media must be shredded or destroyed such that PII cannot be read or otherwise reconstructed, and electronic media must be cleared, purged, or destroyed such that the PII cannot be retrieved. Only the destruction of paper PII, and not redaction, will satisfy the requirements for data destruction. Redaction is specifically excluded as a means of data destruction.
- (c) Upon request Contractor shall provide the EA with a written certification of the secure deletion and/or destruction of PII held by the Contractor or Subcontractors.
- (d) To the extent that Contractor and/or its subcontractors continue to be in possession of any de-identified data (i.e., data that has had all direct and indirect identifiers removed), they agree not to attempt to re-identify de-identified data.

#### **10. Commercial or Marketing Use Prohibition.**

Contractor agrees that it will not sell PII or use or disclose PII for a Commercial or Marketing Purpose.

#### **11. Encryption.**

Contractor shall use industry standard security measures including encryption protocols that comply with New York law and regulations to preserve and protect PII. Contractor must encrypt PII at rest and in transit in accordance with applicable New York laws and regulations.

#### **12. Breach.**

- (a) Contractor shall promptly notify the EA of any Breach of PII without unreasonable delay no later than seven (7) business days after discovery of the Breach. Notifications required pursuant to this section must be in writing, given by personal delivery, e-mail transmission (if contact information is provided for the specific mode of delivery), or by registered or certified, and must to the extent available, include a description of the Breach which includes the date of the incident and the date of discovery; the types of PII affected and the number of records affected; a description of Contractor's investigation; and the contact information for

representatives who can assist the EA. Notifications required by this section must be sent to the EA's District Superintendent or other head administrator with a copy to the Data Protection Office. Violations of the requirement to notify the EA shall be subject to a civil penalty pursuant to Education Law Section 2-d. The Breach of certain PII protected by Education Law Section 2-d may subject the Contractor to additional penalties.

- (b) Notifications required under this paragraph must be provided to the EA at the following address:

**Name:** David Howell

**Title:** Data Protection Officer

**Address:** 8 School Road, P.O. Box 18

**City, State, Zip:** Guilderland Center, NY 12085

**Email:** dataprivacyofficer@guilderlandschools.net

dpo

### **13. Cooperation with Investigations.**

Contractor agrees that it will cooperate with the EA and law enforcement, where necessary, in any investigations into a Breach. Any costs incidental to the required cooperation or participation of the Contractor or its' Authorized Users, as related to such investigations, will be the sole responsibility of the Contractor if such Breach is attributable to Contractor or its Subcontractors.

### **14. Notification to Individuals.**

Where a Breach of PII occurs that is attributable to Contractor, Contractor shall pay for or promptly reimburse the EA for the full cost of the EA's notification to Parents, Eligible Students, teachers, and/or principals, in accordance with Education Law Section 2-d and 8 NYCRR Part 121.

### **15. Termination.**

The confidentiality and data security obligations of the Contractor under this DPA shall survive any termination of this DPA but shall terminate upon Contractor's certifying that it has destroyed all PII.

## **ARTICLE III: PARENT AND ELIGIBLE STUDENT PROVISIONS**

### **1. Parent and Eligible Student Access.**

Education Law Section 2-d and FERPA provide Parents and Eligible Students the right to inspect and review their child's or the Eligible Student's Student Data stored or maintained by the EA. To the extent Student Data is held by Contractor pursuant to the Service Agreement, Contractor shall respond within thirty (30) calendar days to the EA's requests for access to Student Data so the EA can facilitate such review by a Parent or Eligible Student, and facilitate corrections, as necessary. If a Parent or Eligible Student contacts Contractor directly to review any of the Student Data held by Contractor pursuant to the Service Agreement, Contractor shall promptly notify the EA and refer the Parent or Eligible Student to the EA.

## **2. Bill of Rights for Data Privacy and Security.**

As required by Education Law Section 2-d, the Parents Bill of Rights for Data Privacy and Security and the supplemental information for the Service Agreement are included as Exhibit A and Exhibit B, respectively, and incorporated into this DPA. Contractor shall complete and sign Exhibit B and append it to this DPA. Pursuant to Education Law Section 2-d, the EA is required to post the completed Exhibit B on its website.

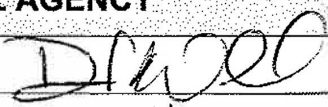
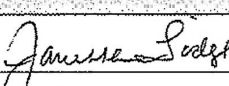
## **ARTICLE IV: MISCELLANEOUS**

### **1. Priority of Agreements and Precedence.**

In the event of a conflict between and among the terms and conditions of this DPA, including all Exhibits attached hereto and incorporated herein and the Service Agreement, the terms and conditions of this DPA shall govern and prevail, shall survive the termination of the Service Agreement in the manner set forth herein, and shall supersede all prior communications, representations, or agreements, oral or written, by the Parties relating thereto.

### **2. Execution.**

This DPA may be executed in one or more counterparts, all of which shall be considered one and the same document, as if all parties had executed a single original document, and may be executed utilizing an electronic signature and/ or electronic transmittal, and each signature thereto shall be and constitute an original signature, as if all parties had executed a single original document.

<b>EDUCATIONAL AGENCY</b>	<b>CONTRACTOR</b>
BY: [Signature] 	BY: 
[Printed Name] DAVID HOWELL	Janessa Lidge
[Title] DATA PROTECTION OFFICER	Contract Administrator
Date: 6/8/2023	Date: 5/16/2023

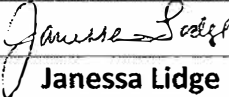
## EXHIBIT A - Education Law §2-d Bill of Rights for Data Privacy and Security

The Guilderland School District, in recognition of the risk of identity theft and unwarranted invasion of privacy, affirms its commitment to safeguarding student personally identifiable information (PII) in educational records from unauthorized access or disclosure in accordance with State and Federal law. The Guilderland School District establishes the following parental bill of rights:

- Student personally identifiable information (PII) will be collected and disclosed only as necessary to achieve educational purposes in accordance with State and Federal Law.
- A student's personally identifiable information cannot be sold or released for any marketing or commercial purposes by the district or any third party contractor. The district will not sell student personally identifiable information and will not release it for marketing or commercial purposes, other than directory information released by the district in accordance with district policy;
- Parents have the right to inspect and review the complete contents of their child's education record (for more information about how to exercise this right, see 5500-R);
- State and federal laws, such as NYS Education Law §2-d and the Family Educational Rights and Privacy Act, protect the confidentiality of students' personally identifiable information. 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;
- A complete list of all student data elements collected by the State Education Department is available for public review at <http://nysed.gov.data-privacy-security> or by writing to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234.
- Parents have the right to have complaints about possible breaches and unauthorized disclosures of student data addressed. Complaints should be directed to Data Privacy Officer, GSCD, PO Box 18, 8 School Road, Guilderland Center, NY 12085, (518) 456-6200; [dataprivacyofficer@guilderlandschools.net](mailto:dataprivacyofficer@guilderlandschools.net). Complaints can also be directed to the New York State Education Department online at <http://nysed.gov.data-privacy-security>, by mail to the Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234 or by email [privacy@mail.nysed.gov](mailto:privacy@mail.nysed.gov) or by telephone at 518-474-0937.
- Parents have the right to be notified in accordance to applicable laws and regulations if a breach or unauthorized release of their student's PII occurs.
- Parents can expect that educational agency workers who handle PII will receive annual training on applicable federal and state laws, regulations, educational agency's policies and safeguards which will be in alignment with industry standards and best practices to protect PII.
- In the event that the District engages a third party provider to deliver student educational services, the contractor or subcontractors will be obligated to adhere to State and Federal Laws and District policy to safeguard student PII. Parents can request information about third party contractors by contacting Data Privacy Officer, GSCD, PO Box 18, 8 School Road, Guilderland Center, NY 12085, (518) 456-6200;



dataprivacyofficer@guilderlandschools.net or can access the information on the district's website,  
www.guilderlandschools.org.

CONTRACTOR	
[Signature]	
[Printed Name]	<b>Janessa Lidge</b>
[Title]	<b>Contract Administrator</b>
Date:	5/16/2023

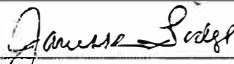
## EXHIBIT B

### BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY - SUPPLEMENTAL INFORMATION FOR CONTRACTS THAT UTILIZE PERSONALLY IDENTIFIABLE INFORMATION

Pursuant to Education Law § 2-d and Section 121.3 of the Commissioner's Regulations, the Educational Agency (EA) is required to post information to its website about its contracts with third-party contractors that will receive Personally Identifiable Information (PII).

<b>Name of Contractor</b>	<b>Desmos Studio PBC</b>
<b>Description of the purpose(s) for which Contractor will receive/access PII</b>	<b>Desmos.com</b>
<b>Type of PII that Contractor will receive/access</b>	Check all that apply: <input checked="" type="checkbox"/> Student PII <input checked="" type="checkbox"/> APPR Data
<b>Contract Term</b>	Contract Start Date <u>5/16/2023</u> Contract End Date <u>5/15/2026</u> <i>JK</i>
<b>Subcontractor Written Agreement Requirement</b>	Contractor will not utilize subcontractors without a written contract that requires the subcontractors to adhere to, at a minimum, materially similar data protection obligations imposed on the contractor by state and federal laws and regulations, and the Contract. (check applicable option)  <input type="checkbox"/> Contractor will not utilize subcontractors. <input checked="" type="checkbox"/> Contractor will utilize subcontractors.
<b>Data Transition and Secure Destruction</b>	Upon expiration or termination of the Contract, Contractor shall: <ul style="list-style-type: none"> <li>Securely transfer data to EA, or a successor contractor at the EA's option and written discretion, in a format agreed to by the parties.</li> <li>Securely delete and destroy data.</li> </ul>
<b>Challenges to Data Accuracy</b>	Parents, teachers or principals who seek to challenge the accuracy of PII will do so by contacting the EA. If a correction to data is deemed necessary, the EA will notify Contractor. Contractor agrees to facilitate such corrections within 21 days of receiving the EA's written request.

<b>Secure Storage and Data Security</b>	<p>Please describe where PII will be stored and the protections taken to ensure PII will be protected: (check all that apply)</p> <p><input checked="" type="checkbox"/> Using a cloud or infrastructure owned and hosted by a third party.</p> <p><input type="checkbox"/> Using Contractor owned and hosted solution</p> <p><input type="checkbox"/> Other:</p> <p>Please describe how data security and privacy risks will be mitigated in a manner that does not compromise the security of the data:</p> <p>Desmos maintains a comprehensive information security plan that details the various technical and administrative protections in place throughout different parts of our information systems. These safeguards are regularly evaluated, and Desmos employees with access to user data are trained in their application.</p>
<b>Encryption</b>	Data will be encrypted while in motion and at rest.

<b>CONTRACTOR</b>	
<b>[Signature]</b>	
<b>[Printed Name]</b>	<b>Janessa Lidge</b>
<b>[Title]</b>	<b>Contract Administrator</b>
<b>Date:</b>	5/16/2023

## EXHIBIT C - 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.	Desmos maintains a written information security plan that includes administrative and technical safeguards for personal information in our various systems. Specific aspects of these safeguards are outlined in questions below.
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	Personal information is only ever stored electronically, and never on mobile devices or removable media. Access to personal information is protected by strong passwords and multi-factor authentication. Any local machine used to temporarily store personal information must have full-disk encryption enabled; data must be stored for the minimum time necessary, and it must either be held in volatile memory or securely deleted afterward. Persistent storage of personal information is handled by a list of approved, industry-standard subcontractors (e.g., Amazon Web Services), where it is encrypted both in transit and at rest.
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.	At the time of hiring, employees with access to personal information receive training on the appropriate handling of personal information and the company's written information security plan. Current employees receive refresher training annually.
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.	Employee contracts include provisions for compliance with company policies, including those relating to the handling of personal information. Violation of these policies may result in disciplinary measures. Employees with access to personal information must undergo a background check at the time of hiring. Desmos uses industry-standard subcontractors for hosted data storage

		(e.g., Amazon Web Services), and reviews those agreements annually or when there is a material change.
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.	The written information security plan addresses data breach response, including (1) determining the extent of a breach and which types of information were accessed, (2) limiting the scope of a breach in progress, (3) making notification to required entities, (4) postmortem analysis, and (5) remediation. Desmos logs access to personal information and employs passive intrusion detection.
6	Describe how data will be transitioned to the EA when no longer needed by you to meet your contractual obligations, if applicable.	Data will not be transitioned to the EA. If the user or EA requests an account deletion, all data associated with that account will be permanently deleted within 60 days.
7	Describe your secure destruction practices and how certification will be provided to the EA.	Upon account termination, Desmos will delete any information associated with that account from its hosted permanent data stores. Any derived data (e.g., in log files) will likewise be deleted within 60 days. Desmos can provide written confirmation of account deletion upon request.
8	Outline how your data security and privacy program/practices align with the EA's applicable policies.	The company's written information security plan includes provisions for handling personally identifiable information and breach response and notification (as discussed below).
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.

## EXHIBIT C.1 – 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)	<b>Asset Management (ID.AM):</b> 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.	Desmos maintains minimal physical devices—only for development and testing. Software platforms are inventoried as part of the development process. External information systems are mapped and catalogued as part of the normal operations cycle. Specific, formal cybersecurity roles exist for a small subset of the engineering team. Cybersecurity expectations for the entire workforce are established during employee onboarding and/or annual training in the form of the written information security plan. As a small team, Desmos does not map organizational communication or data flows as a general rule.
	<b>Business Environment (ID.BE):</b> 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.	The company's role in the educational technology space, along with its organizational goals and mission, are reviewed and communicated at least quarterly. Our critical functions, dependencies for critical services, and resilience requirements for various operating states are identified as part of the normal development and operations cycle.
	<b>Governance (ID.GV):</b> 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.	Specific, formal cybersecurity roles exist for a small subset of the engineering team. Cybersecurity expectations for the entire workforce are established during employee onboarding and/or annual training in the form of the written information security plan. This training also includes the company's and employees' responsibilities under applicable laws and regulations (e.g., COPPA, FERPA).
	<b>Risk Assessment (ID.RA):</b> The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	Vulnerabilities are identified and documented as part of the software review process, as well as through automated dependency audits. Business impacts are considered in the determination of vulnerability severity. Vulnerabilities are prioritized when identified.
	<b>Risk Management Strategy (ID.RM):</b> The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	Risk management and risk tolerance determinations are included in everyday engineering practices—for both infrastructure and software.
	<b>Supply Chain Risk Management (ID.SC):</b> 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.	Agreements with and policies of subcontractors are reviewed annually. Critical data is stored in redundant systems
PROTECT (PR)	<b>Identity Management, Authentication and Access Control (PR.AC):</b> 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.	Access to digital personal information is controlled by setting the appropriate permissions on Desmos employee accounts with our various data storage services. Accounts with access to personal information are only granted to current Desmos employees who have undergone a background check, and permission levels are set by account administrators based on what kind of information an employee needs in order to fulfill their role on the team. Accounts with access to personal information are required to use multi-factor authentication, which is enforced by Desmos administrators.
	<b>Awareness and Training (PR.AT):</b> 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.	Desmos employees receive information security training at the time of hiring and refresher training annually.

Function	Category	Contractor Response
	<b>Data Security (PR.DS):</b> Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	Personal information is encrypted both in transit and at rest. Desmos employs auto-scaling policies to ensure adequate availability in the face of increased demand (whether legitimate or malicious). Development and testing environments are separate from production. Identify/persistence is managed through a separate back-end service with its own redundant backups.
	<b>Information Protection Processes and Procedures (PR.IP):</b> 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.	Snapshots of critical data are regularly backed up, and point-in-time restores are possible. The written information security plan includes incident response procedures. Data removed by users, as well as derived data (e.g. logs) is deleted from Desmos systems within 60 days. Vulnerability management is a regular part of the development/operations cycle.
	<b>Maintenance (PR.MA):</b> Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	Remote maintenance of Desmos systems is approved by Desmos administrators and performed in a manner that prevents unauthorized access.
	<b>Protective Technology (PR.PT):</b> Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	Desmos maintains audit records and access logs of queries for personal information. Personal information is not permitted to be stored on removable media. Load balancing and autoscaling strategies ensure resiliency to both normal and adverse usage situations.
<b>DETECT (DE)</b>	<b>Anomalies and Events (DE.AE):</b> Anomalous activity is detected and the potential impact of events is understood.	Desmos has configured alarms relative to baseline network operations to alert engineers when critical thresholds are exceeded.
	<b>Security Continuous Monitoring (DE.CM):</b> The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	Desmos continuously monitors network events and employs passive intrusion protection for critical system components.
	<b>Detection Processes (DE.DP):</b> Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	On-call responsibilities for engineers detecting and responding to anomalous events are clearly defined. Event detection information is communicated by both automated and interpersonal means.
<b>RESPOND (RS)</b>	<b>Response Planning (RS.RP):</b> Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.	The written information security plan includes incident response.
	<b>Communications (RS.CO):</b> Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	The company's incident response plan defines employee roles and responsibilities and requirements for coordination among teams.
	<b>Analysis (RS.AN):</b> Analysis is conducted to ensure effective response and support recovery activities.	All notifications from detection systems are investigated and reported. Vulnerability disclosures are triaged and addressed as part of normal development and operations.
	<b>Mitigation (RS.MI):</b> Activities are performed to prevent expansion of an	The company's incident response plan includes steps to minimize the impact of an incident by limiting its spread to yet-unaffected systems.

Function	Category	Contractor Response
RECOVER (RC)	event, mitigate its effects, and resolve the incident.	
	<b>Improvements (RS.IM):</b> Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	All significant incidents receive postmortem analysis during engineering review and are used to improve existing policies, procedures, and infrastructure/software decisions.
	<b>Recovery Planning (RC.RP):</b> Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.	The company's incident response plan includes recovery.
	<b>Improvements (RC.IM):</b> Recovery planning and processes are improved by incorporating lessons learned into future activities.	The company's incident response plan includes postmortem analysis of any incident that requires recovery operations.
	<b>Communications (RC.CO):</b> 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 company's incident response plan includes communication requirements for both internal and external stakeholders. Team members responsible for business and public relations concerns are included in that communication plan.