Remind Data Security and Privacy Plan

Policy Statement

This document explains Remind's Information Security Management System (ISMS) and information security (infosec) governance efforts within the organization that are relevant to the state, federal, and local data security and privacy contract requirements set forth by the New York Department of Education for subcontractors. Remind will maintain and review this Data Security and Privacy Plan, no less than annually, with the objective of demonstrating the approach for ongoing compliance with these requirements.

Scope

This policy applies to all Remind employees, contractors, and third parties ("users") using its electronic resources, and is part of the Remind corporate information security policy to support active agreements with organizations and educational institutions in the state of New York.

Personnel Training

Remind is required by regulation and law to protect the personally identifiable information and personal data of all of our users no matter their ages. Remind requires employees to receive privacy training at the time of hire and on a regular basis thereafter, no less than annually, to ensure their understanding of the relevant regulations and laws that Remind must comply with. These laws include:

- Various US states' student privacy laws including, without limitation, New York State Education Law § 2-d ("New York Ed. 2-d), and Section 121 of New York regulations that implement that law and related law.
- The Family Educational Rights Privacy Act (FERPA);
- The Children's Online Privacy Protection Act (COPPA); and,
- European Union General Data Protection Regulation.

Supplier Management

Supplier management practices must be consistent with Remind's Vendor Risk Management Policy, including the following key activities.

New Vendors

Prior to engaging any new vendors or suppliers, Remind reviews their security and privacy to determine whether the vendor or supplier practices satisfy our standards and our legal and contractual commitments. Once the vendor has been categorized based on the nature of the service, a review of the vendor's security relative to the corresponding risk tier is to be done prior to sharing any Remind or customer data with the vendor.

Remind requires that contractual terms with new vendors must include, at a minimum, requisite data protection requirements and the return or destruction of all Remind data upon termination of vendor services consistent with language contained in the Remind Data Processing Addendum.

Vendor Oversight and Monitoring
A risk-based approach is taken for vendor security oversight, where more rigor and in-depth analysis are applied to vendors with whom sensitive data is exchanged. All vendors are subject to an annual review of security, but different focus and scrutiny are directed to different vendor tiers.

Terminating Vendor Relationships
Upon termination, procurement and operations personnel are to immediately ensure active data transfers of Remind data cease, and access to Remind information systems is revoked.

Information Security Incident Management

The handling of information security incidents will be consistent with Remind's confidential Security Incident Response Plan, including processes to support:

- Detection of security incidents
- Classification of security incidents
- Steps to verify, contain, investigate, mitigate and recover
- Incident report documentation
- Any additional technical or procedural efforts required to prevent a subsequent incident

Legal Compliance
Consistent with Remind's corporate security policy, and other applicable laws and regulations, the vendor or supplier may be required to notify regulatory and law enforcement agencies, as well as its customers, of incidents involving unauthorized access to or use of customer or employee information, etc. Remind shall comply with all notice requirements under the security guidelines. Remind's legal department will consult with other representatives, as necessary, to determine whether, and which agencies must receive notice, as well as the manner, content, and timing of delivery of such notices, based on certain standards. To the extent necessary, Remind may elect to consult with internal and external counsel.

The requirement should include but are not limited to the following parties (if applicable):

- Regulatory agencies
- Law enforcement
- Federal Bureau of Investigation
- Local police department
- Customers
- Remind users

- Service providers or third parties (if any)

Depending on the nature of the threat and assessed risk, “Standards” for providing notice(s) as a whole or just to those impacted may be used (limited notices)

Data Retention and Destruction

Remind will either delete or return, within a commercially reasonable period of time but not to exceed 45 days, all personally identifiable information upon the expiration of any agreement when requested to do so in writing by notification, as that term is defined in Remind’s contract with the contracting party, from the contracting party.

General Controls

Remind has adopted ISO/IEC 27001 and ISO/IEC 27002 as a framework for the design and monitoring of administrative, operational, and technical safeguards to maintain integrity, availability, and confidentiality of personally identifiable information.

To demonstrate how Remind’s ISMS is consistent with the NIST Cybersecurity Framework V1.1, a bridge mapping for the control is defined as follows.

Category	Subcategory	Informative References
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 business objectives and the organization’s risk strategy.	**ID.AM-1**: Physical devices and systems within the organization are inventoried	**ISO/IEC 27001:2013** A.8.1.1, A.8.1.2
	ID.AM-2: Software platforms and applications within the organization are inventoried	**ISO/IEC 27001:2013** A.8.1.1, A.8.1.2
	ID.AM-3: Organizational communication and data flows are mapped	**ISO/IEC 27001:2013** A.13.2.1
	ID.AM-4: External information systems are catalogued	**ISO/IEC 27001:2013** A.11.2.6
	ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	**ISO/IEC 27001:2013** A.8.2.1
	ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	**ISO/IEC 27001:2013** A.6.1.1

Category	Subcategory	Informative References
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.	**ID.BE-1:** The organization's role in the supply chain is identified and communicated	**ISO/IEC 27001:2013** A.15.1.3, A.15.2.1, A.15.2.2
	ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	N/A - Remind is not a critical infrastructure organization. Remind is a Software-as-a-Service 2-Way Communication Platform that supports educators, students, and parents.
	ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	Remind's vision, mission and values are communicated to staff and stakeholders.
	ID.BE-4: Dependencies and critical functions for delivery of critical services are established	**ISO/IEC 27001:2013** A.11.2.2, A.11.2.3, A.12.1.3
	ID.BE-5: Resilience requirements to support delivery of critical services are established	**ISO/IEC 27001:2013** A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1
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.	**ID.GV-1:** Organizational information security policy is established	**ISO/IEC 27001:2013** A.5.1.1
	ID.GV-2: Information security roles & responsibilities are coordinated and aligned with internal roles and external partners	**ISO/IEC 27001:2013** A.6.1.1, A.7.2.1
	ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	**ISO/IEC 27001:2013** A.18.1
	ID.GV-4: Governance and risk management processes address cybersecurity risks	**ISO/IEC 27001:2013** Clause 8.3
Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	**ID.RA-1:** Asset vulnerabilities are identified and documented	**ISO/IEC 27001:2013** A.12.6.1, A.18.2.3
	ID.RA-2: Threat and vulnerability information is received from information sharing forums and sources	**ISO/IEC 27001:2013** A.6.1.4
	ID.RA-3: Threats, both internal and external, are identified and documented	**ISO/IEC 27001:2013** Clause 8.2

Category	Subcategory	Informative References
Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	**ID.RA-4:** Potential business impacts and likelihoods are identified	**ISO/IEC 27001:2013** Clause 8.2
	ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	**ISO/IEC 27001:2013** A.12.6.1
	ID.RA-6: Risk responses are identified and prioritized	**ISO/IEC 27001:2013** Clause 8.2
Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	**ID.RM-1:** Risk management processes are established, managed, and agreed to by organizational stakeholders	**ISO/IEC 27001:2013** Clause 6.1.2
	ID.RM-2: Organizational risk tolerance is determined and clearly expressed	**ISO/IEC 27001:2013** Clause 6.1.2, Clause 8.2
	ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis	N/A - Remind is not a critical infrastructure organization. Remind is a Software-as-a-Service 2-Way Communication Platform that supports educators, students, and parents.
Access Control (PR.AC): Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	**PR.AC-1:** Identities and credentials are managed for authorized devices and users	**ISO/IEC 27001:2013** A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3
	PR.AC-2: Physical access to assets is managed and protected	**ISO/IEC 27001:2013** A.11.1.1, A.11.1.2, A.11.1.4, A.11.1.6, A.11.2.3
	PR.AC-3: Remote access is managed	**ISO/IEC 27001:2013** A.6.2.2, A.13.1.1, A.13.2.1
	PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties	**ISO/IEC 27001:2013** A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4
	PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate	**ISO/IEC 27001:2013** A.13.1.1, A.13.1.3, A.13.2.1

Category	Subcategory	Informative References
Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.	**PR.AT-1:** All users are informed and trained	**ISO/IEC 27001:2013** A.7.2.2
	PR.AT-2: Privileged users understand roles & responsibilities	**ISO/IEC 27001:2013** A.6.1.1, A.7.2.2
	PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities	**ISO/IEC 27001:2013** A.6.1.1, A.7.2.2
	PR.AT-4: Senior executives understand roles & responsibilities	**ISO/IEC 27001:2013** A.6.1.1, A.7.2.2,
	PR.AT-5: Physical and information security personnel understand roles & responsibilities	**ISO/IEC 27001:2013** A.6.1.1, A.7.2.2,
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.	**PR.DS-1:** Data-at-rest is protected	**ISO/IEC 27001:2013** A.8.2.3
	PR.DS-2: Data-in-transit is protected	**ISO/IEC 27001:2013** A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3
	PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition	**ISO/IEC 27001:2013** A.8.2.3, A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.7
	PR.DS-4: Adequate capacity to ensure availability is maintained	**ISO/IEC 27001:2013** A.12.3.1
	PR.DS-5: Protections against data leaks are implemented	**ISO/IEC 27001:2013** A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3
	PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	**ISO/IEC 27001:2013** A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3
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.	**PR.DS-7:** The development and testing environment(s) are separate from the production environment	**ISO/IEC 27001:2013** A.12.1.4

Category	Subcategory	Informative References
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.	**PR.IP-1:** A baseline configuration of information technology/industrial control systems is created and maintained	**ISO/IEC 27001:2013** A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4
	PR.IP-2: A System Development Life Cycle to manage systems is implemented	**ISO/IEC 27001:2013** A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.5
	PR.IP-3: Configuration change control processes are in place	**ISO/IEC 27001:2013** A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4
	PR.IP-4: Backups of information are conducted, maintained, and tested periodically	**ISO/IEC 27001:2013** A.12.3.1, A.17.1.2A.17.1.3, A.18.1.3
	PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met	**ISO/IEC 27001:2013** A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3
	PR.IP-6: Data is destroyed according to policy	**ISO/IEC 27001:2013** A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7
	PR.IP-7: Protection processes are continuously improved	**ISO/IEC 27001:2013** Clause 9.1, A.18.2.2
	PR.IP-8: Effectiveness of protection technologies is shared with appropriate parties	**ISO/IEC 27001:2013** A.16.1.6
	PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	**ISO/IEC 27001:2013** A.16.1.1, A.17.1.1, A.17.1.2
	PR.IP-10: Response and recovery plans are tested	**ISO/IEC 27001:2013** A.17.1.3
	PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	**ISO/IEC 27001:2013** A.7.1.1, A.7.3.1, A.8.1.4
	PR.IP-12: A vulnerability management plan is developed and implemented	**ISO/IEC 27001:2013** A.12.6.1, A.18.2.2

Category	Subcategory	Informative References
Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.	**PR.MA-1:** Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools	**ISO/IEC 27001:2013** A.11.1.2, A.11.2.4, A.11.2.5
	PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	**ISO/IEC 27001:2013** A.11.2.4, A.15.1.1, A.15.2.1
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.	**PR.PT-1:** Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	**ISO/IEC 27001:2013** A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1
	PR.PT-2: Removable media is protected and its use restricted according to policy	**ISO/IEC 27001:2013** A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.9
	PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality	**ISO/IEC 27001:2013** A.9.1.2
	PR.PT-4: Communications and control networks are protected	**ISO/IEC 27001:2013** A.13.1.1, A.13.2.1
Anomalies and Events (DE.AE): Anomalous activity is detected in a timely manner and the potential impact of events is understood.	**DE.AE-1:** A baseline of network operations and expected data flows for users and systems is established and managed	**ISO/IEC 27001:2013** A.12.1.4, A.14.2.5
	DE.AE-2: Detected events are analyzed to understand attack targets and methods	**ISO/IEC 27001:2013** A.16.1.1, A.16.1.4
	DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors	**ISO/IEC 27001:2013** A.12.4.1
	DE.AE-4: Impact of events is determined	**ISO/IEC 27001:2013** A.16.1.4, A.16.1.5
	DE.AE-5: Incident alert thresholds are established	**ISO/IEC 27001:2013** A.16.1.4, A.16.1.5
Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.	**DE.CM-1:** The network is monitored to detect potential cybersecurity events	**ISO/IEC 27001:2013** A.12.4.1, A.13.1.1
	DE.CM-2: The physical environment is monitored to detect potential cybersecurity events	**ISO/IEC 27001:2013** A.11.1.3, A.11.1.5
	DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events	**ISO/IEC 27001:2013** A.12.4.1

Category	Subcategory	Informative References
Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.	**DE.CM-4:** Malicious code is detected	**ISO/IEC 27001:2013** A.12.2.1
	DE.CM-5: Unauthorized mobile code is detected	**ISO/IEC 27001:2013** A.12.5.1
	DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events	**ISO/IEC 27001:2013** A.14.2.7, A.15.2.1
	DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	**ISO/IEC 27001:2013** A.11.1.3, A.12.4.1
	DE.CM-8: Vulnerability scans are performed	**ISO/IEC 27001:2013** A.12.6.1
Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.	**DE.DP-1:** Roles and responsibilities for detection are well defined to ensure accountability	**ISO/IEC 27001:2013** A.6.1.1
	DE.DP-2: Detection activities comply with all applicable requirements	**ISO/IEC 27001:2013** A.18.1.4
	DE.DP-3: Detection processes are tested	**ISO/IEC 27001:2013** A.14.2.8
	DE.DP-4: Event detection information is communicated to appropriate parties	**ISO/IEC 27001:2013** A.16.1.2
	DE.DP-5: Detection processes are continuously improved	**ISO/IEC 27001:2013** A.16.1.6
Response Planning (RS.RP): Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events.	**RS.RP-1:** Response plan is executed during or after an event	**ISO/IEC 27001:2013** A.16.1.5
Communications (RS.CO): Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.	**RS.CO-1:** Personnel know their roles and order of operations when a response is needed	**ISO/IEC 27001:2013** A.6.1.1, A.16.1.1
	RS.CO-2: Events are reported consistent with established criteria	**ISO/IEC 27001:2013** A.6.1.3, A.16.1.2
	RS.CO-3: Information is shared consistent with response plans	**ISO/IEC 27001:2013** A.16.1.2

Category	Subcategory	Informative References
Communications (RS.CO): Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.	**RS.CO-4:** Coordination with stakeholders occurs consistent with response plans	**ISO/IEC 27001:2013** A.16.1.1
	RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	**ISO/IEC 27001:2013** A.6.1.3, A.6.1.4
Analysis (RS.AN): Analysis is conducted to ensure adequate response and support recovery activities.	**RS.AN-1:** Notifications from detection systems are investigated	**ISO/IEC 27001:2013** A.12.4.1, A.12.4.3, A.16.1.5
	RS.AN-2: The impact of the incident is understood	**ISO/IEC 27001:2013** A.16.1.6
	RS.AN-3: Forensics are performed	**ISO/IEC 27001:2013** A.16.1.7
	RS.AN-4: Incidents are categorized consistent with response plans	**ISO/IEC 27001:2013** A.16.1.4
Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.	**RS.MI-1:** Incidents are contained	**ISO/IEC 27001:2013** A.16.1.5
	RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks	**ISO/IEC 27001:2013** A.12.6.1
Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	**RS.IM-1:** Response plans incorporate lessons learned	**ISO/IEC 27001:2013** A.16.1.6
	RS.IM-2: Response strategies are updated	**ISO/IEC 27001:2013** A.5.1.2, A.16.1.6
Recovery Planning (RC.RP): Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.	**RC.RP-1:** Recovery plan is executed during or after an event	**ISO/IEC 27001:2013** A.16.1.5
Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	**RC.IM-1:** Recovery plans incorporate lessons learned	**ISO/IEC 27001:2013** A.16.1.1, 17.1.1
	RC.IM-2: Recovery strategies are updated	**ISO/IEC 27001:2013** A.17.1.1

Category	Subcategory	Informative References
Communications (RC.CO): Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors.	**RC.CO-1:** Public relations are managed	**ISO/IEC 27001:2013** A.16.1.1
	RC.CO-2: Reputation after an event is repaired	**ISO/IEC 27001:2013** A.16.1.1
	RC.CO-3: Recovery activities are communicated to internal stakeholders and executive and management teams	**ISO/IEC 27001:2013** A.16.1.1

Referenced Policies

Information Security Management Systems Policy
Security Incident Response Plan
Vendor Risk Management

Date Reviewed	Date Published	Version	Approver Name, Title
5/4/2020	5/4/2020	1.0	Emily McDonnell, Head of Trust and Safety Winston Wu, VP, Finance Barak Engel, CISO