

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 (including as set forth by the New York Department of Education for subcontractors).

Scope

This policy applies to all Remind employees, contractors, and third parties (“users”) using its electronic resources, and is part of the Remind Information Security Management System to support active agreements with organizations and educational institutions in the state of New York and other educational organizations in US states observing the NIST cybersecurity framework.

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 vendor or supplier, an initial review will be conducted to evaluate the risk they pose and their criticality to the services we provide. Once the vendor has been categorized based on the nature of the service, review of the vendor’s security and privacy relative to the corresponding risk tiers is to be done prior to engaging with the vendor.

As a best practice, it is recommended that contractual terms with new vendors, especially high risk vendors with access to Remind customer data, require the return or destruction of all Remind data upon termination of vendor services.

Vendor Oversight and Monitoring

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

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 Information Security Management System, 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 90 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 27001:2022 5.9
	ID.AM-2: Software platforms and applications within the organization are inventoried	ISO/IEC 27001:2022 5.9
	ID.AM-3: Organizational communication and data flows are mapped	ISO/IEC 27001:2022 5.14
	ID.AM-4: External information systems are catalogued	ISO/IEC 27001:2022 7.9
	ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	ISO/IEC 27001:2022 5.12
	ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	ISO/IEC 27001:2022 5.2
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 27001:2022 5.21, 5.22
	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 Education 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 27001:2022 7.4, 7.11, 7.12, 8.6
	ID.BE-5: Resilience requirements to support delivery of critical services are established	ISO/IEC 27001:2022 7.5, 5.29, 8.14
Category	Subcategory	Informative References
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 27001:2022 5.1
	ID.GV-2: Information security roles & responsibilities are coordinated and aligned with internal roles and external partners	ISO/IEC 27001:2022 5.2, 5.4
	ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	ISO/IEC 27001:2022 5.31,5.32,5.33
	ID.GV-4: Governance and risk management processes address cybersecurity risks	ISO/IEC 27001:2022 7.10
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 27001:2022 8.8
	ID.RA-2: Threat and vulnerability information is received from information sharing forums and sources	ISO/IEC 27001:2022 8.16, 5.7
	ID.RA-3: Threats, both internal and external, are identified and documented	ISO/IEC 27001:2022 5.10, 5.12, 5.13
	ID.RA-4: Potential business impacts and likelihoods are identified	ISO/IEC 27001:2022 5.10, 5.12, 5.13
	ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	ISO/IEC 27001:2022 8.8

Category	Subcategory	Informative References
	ID.RA-6: Risk responses are identified and prioritized	ISO/IEC 27001:2022 5.10, 5.12, 5.13
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 27001:2022 8.1
	ID.RM-2: Organizational risk tolerance is determined and clearly expressed	ISO/IEC 27001:2022 5.10, 5.12, 5.13, 8.1
	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 Education 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 27001:2022 5.16, 5.17, 5.18, 8.5
	PR.AC-2: Physical access to assets is managed and protected	ISO/IEC 27001:2022 7.1,7.2,7.3,7.4, 7.12
	PR.AC-3: Remote access is managed	ISO/IEC 27001:2022 5.14, 6.7, 8.20
	PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties	ISO/IEC 27001:2022 5.15, 6.8, 8.2, 8.3, 8.18
	PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate	ISO/IEC 27001:2022 5.14, 8.20, 8.22
	PR.AC-6: Identities are proofed and bound to credentials, and asserted in interactions when appropriate	ISO/IEC 27001:2022 5.29, 6.8, 5.15, 5.18, 8.2, 8.3. 8.18
Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity	PR.AT-1: All users are informed and trained	ISO/IEC 27001:2022 6.3
	PR.AT-2: Privileged users	ISO/IEC 27001:2022 5.2, 6.3

awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.	understand roles & responsibilities	
	PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities	ISO/IEC 27001:2022 5.2, 6.3
	PR.AT-4: Senior executives understand roles & responsibilities	ISO/IEC 27001:2022 5.2, 6.3
	PR.AT-5: Physical and information security personnel understand roles & responsibilities	ISO/IEC 27001:2022 7.4
Category	Subcategory	Informative References
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 27001:2022 8.8
	PR.DS-2: Data-in-transit is protected	ISO/IEC 27001:2022 5.10, 8.20, 5.14, 8.26
	PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition	ISO/IEC 27001:2022 8.8, 7.10, 7.14
	PR.DS-4: Adequate capacity to ensure availability is maintained	ISO/IEC 27001:2022 8.13
	PR.DS-5: Protections against data leaks are implemented	ISO/IEC 27001:2022 5.3, 6.1, 6.2, 6.5, 5.13, 5.10, 5.15, 8.2, 8.3, 8.17, 8.4, 8.22, 5.14, 8.26
	PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	ISO/IEC 27001:2022 8.7, 8.19, 8.26
	PR.DS-7: The development and testing environment(s) are separate from the production environment	ISO/IEC 27001:2022 8.31
	PR.DS-8: Integrity checking mechanisms are used to verify hardware integrity	ISO/IEC 27001:2022 7.13
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	PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained	ISO/IEC 27001:2022 8.32, 8.9, 8.19
	PR.IP-2: A System Development Life Cycle to manage systems is implemented	ISO/IEC 27001:2022 5.8, 8.25, 8.27
	PR.IP-3: Configuration change control processes are in place	ISO/IEC 27001:2022 8.32, 8.9, 8.19

information systems and assets.	PR.IP-4: Backups of information are conducted, maintained, and tested periodically	ISO/IEC 27001:2022 8.13, 5.29, 5.33
	PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met	ISO/IEC 27001:2022 7.4, 7.5, 7.11, 7.12
	PR.IP-6: Data is destroyed according to policy	ISO/IEC 27001:2022 8.8, 7.10, 7.14
	PR.IP-7: Protection processes are continuously improved	ISO/IEC 27001:2022 5.15, 5.36
	PR.IP-8: Effectiveness of protection technologies is shared with appropriate parties	ISO/IEC 27001:2022 5.27
	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 27001:2022 5.24, 5.29, 5.3
	PR.IP-10: Response and recovery plans are tested	ISO/IEC 27001:2022 5.3
	PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	ISO/IEC 27001:2022 6.1, 6.5, 5.34
	PR.IP-12: A vulnerability management plan is developed and implemented	ISO/IEC 27001:2022 8.8, 5.36
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 27001:2022 7.2, 7.10, 7.13
	PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	ISO/IEC 27001:2022 7.13, 5.19, 5.22

<p>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.</p>	<p>PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy</p>	<p>ISO/IEC 27001:2022 8.15, 8.17, 8.34</p>
	<p>PR.PT-2: Removable media is protected and its use restricted according to policy</p>	<p>ISO/IEC 27001:2022 5.1, 5.10, 7.7, 7.10</p>
	<p>PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality</p>	<p>ISO/IEC 27001:2022 5.15</p>
	<p>PR.PT-4: Communications and control networks are protected</p>	<p>ISO/IEC 27001:2022 8.20, 5.14</p>
	<p>PR.PT-5: Systems operate in pre-defined functional states to achieve availability (e.g. under duress, under attack, during recovery, normal operations).</p>	<p>ISO/IEC 27001:2022 5.29, 8.14</p>
Category	Subcategory	Informative References
<p>Anomalies and Events (DE.AE): Anomalous activity is detected in a timely manner and the potential impact of events is understood.</p>	<p>DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed</p>	<p>ISO/IEC 27001:2022 8.16</p>
	<p>DE.AE-2: Detected events are analyzed to understand attack targets and methods</p>	<p>ISO/IEC 27001:2022 5.24, 5.25</p>
	<p>DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors</p>	<p>ISO/IEC 27001:2022 8.15</p>
	<p>DE.AE-4: Impact of events is determined</p>	<p>ISO/IEC 27001:2022 5.25, 5.26</p>
	<p>DE.AE-5: Incident alert thresholds are established</p>	<p>ISO/IEC 27001:2022 5.25, 5.26</p>
<p>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.</p>	<p>DE.CM-1: The network is monitored to detect potential cybersecurity events</p>	<p>ISO/IEC 27001:2022 8.16</p>
	<p>DE.CM-2: The physical environment is monitored to detect potential cybersecurity events</p>	<p>ISO/IEC 27001:2022 7.4</p>
	<p>DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events</p>	<p>ISO/IEC 27001:2022 8.15</p>
	<p>DE.CM-4: Malicious code is detected</p>	<p>ISO/IEC 27001:2022 8.7</p>

	DE.CM-5: Unauthorized mobile code is detected	ISO/IEC 27001:2022 8.16, 8.19
	DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events	ISO/IEC 27001:2022 8.30, 5.22
	DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	ISO/IEC 27001:2022 8.16
	DE.CM-8: Vulnerability scans are performed	ISO/IEC 27001:2022 8.8
Category	Subcategory	Informative References
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 27001:2022 5.2
	DE.DP-2: Detection activities comply with all applicable requirements	ISO/IEC 27001:2022 5.34
	DE.DP-3: Detection processes are tested	ISO/IEC 27001:2022 8.29
	DE.DP-4: Event detection information is communicated to appropriate parties	ISO/IEC 27001:2022 6.8
	DE.DP-5: Detection processes are continuously improved	ISO/IEC 27001:2022 5.27
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 27001:2022 5.26
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 27001:2022 5.2, 5.24
	RS.CO-2: Events are reported consistent with established criteria	ISO/IEC 27001:2022 6.8
	RS.CO-3: Information is shared consistent with response plans	ISO/IEC 27001:2022 6.8
	RS.CO-4: Coordination with	ISO/IEC 27001:2022 5.24

	stakeholders occurs consistent with response plans	
	RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	ISO/IEC 27001:2022 5.5, 5.6
Category	Subcategory	Informative References
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 27001:2022 8.15, 8.16, 5.26
	RS.AN-2: The impact of the incident is understood	ISO/IEC 27001:2022 5.27
	RS.AN-3: Forensics are performed	ISO/IEC 27001:2022 5.28
	RS.AN-4: Incidents are categorized consistent with response plans	ISO/IEC 27001:2022 5.25
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 27001:2022 5.26
	RS.MI-2: Incidents are mitigated	ISO/IEC 27001:2022 8.7, 5.26
	RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks	ISO/IEC 27001:2022 8.8
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 27001:2022 5.27
	RS.IM-2: Response strategies are updated	ISO/IEC 27001:2022 5.1, 6.27
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 27001:2022 5.26
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 27001:2022 5.24, 5.29
	RC.IM-2: Recovery strategies are updated	ISO/IEC 27001:2022 5.29

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 27001:2022 5.24
	RC.CO-2: Reputation after an event is repaired	ISO/IEC 27001:2022 5.24
	RC.CO-3: Recovery activities are communicated to internal stakeholders and executive and management teams	ISO/IEC 27001:2022 5.24
Category	Subcategory	Informative References
Supply Chain 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 in place the processes to identify, assess and manage supply chain risks. 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 in place the processes to identify, assess and manage supply chain risks.	ID.SC-1: Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders	ISO/IEC 27001:2022 5.19, 5.20, 5.21, 5.22
	ID.SC-2: Identify, prioritize and assess suppliers and partners of critical information systems, components and services using a cyber supply chain risk assessment process (Onboarding for Critical Suppliers and Due Diligence)	ISO/IEC 27001:2022 5.22
	ID.SC-3: Suppliers and partners are required by contract to implement appropriate measures designed to meet the objectives of the Information Security program or Cyber Supply Chain Risk Management Plan.	ISO/IEC 27001:2022 5.19, 5.20, 5.21
	ID.SC-4: Suppliers and partners are monitored to confirm that they have satisfied their obligations as required. Reviews of audits, summaries of test results, or other equivalent evaluations of suppliers/providers are conducted (Right toe Audit and NDA)	ISO/IEC 27001:2022 5.22
	ID.SC-5: Response and recovery planning and testing are conducted with critical suppliers/providers	ISO/IEC 27001:2022 5.29