Akindi Data & Security

This Data Classification Policy outlines how data is classified, handled, and stored, and accessed within Akindi.

Akindi Inc.

480 Adelaide St. W
Toronto, ON, M5V 1T2

www.akindi.com

Data Classification Categories

Public Data: Information intended for public consumption, with no restrictions on access or distribution. Akindi's Public data includes product features and functionality, marketing materials, and release notes.

Internal Data: Information intended for internal use within the organization, which is only accessible to Akindi employees. Akindi's internal data include product technical specifications, company policies and procedures.

Personal Identifiable Information: Akindi collects and stores instructor name and email, student name, email, and identification number.

Confidential Data: Information that requires heightened protection due to its sensitive nature. Access to confidential data is restricted to authorized personnel only which includes customer data such as PII, student test sheets, grades, and answer key data.

Data Handling and Storage

Ownership: User Data is and shall remain the sole and exclusive property of the user and all right, title, and interest in it is reserved by the user.

Encryption: Confidential and sensitive data is encrypted both in transit and at rest to prevent unauthorized access or interception.

All data sent to or from Akindi is encrypted in transit using 256-bit encryption. Data is encrypted in the block storage system with AES 256 data-at-rest encryption with integrated key management. Data-at-rest encryption is also provided in the Swift object storage system.

Akindi Data & Security

Akindi Inc.

480 Adelaide St. W
Toronto, ON, M5V 1T2

www.akindi.com

All of Akindi's external communication is secured with HTTPS. The SSL terminator, haproxy, is configured to:

- Redirect (HTTP 301) all insecure (HTTP) traffic to HTTPS
- Use HSTS to prevent downgrade attacks
- Use a 2048 bit key
- Use only TLS 1.3 and above (SSLv2 and SSLv3 are explicitly disabled) Disable insecure cipher suites

Data Residency: All Customer Data is stored and processed exclusively in Google Cloud data centres located in Canada (Toronto or Montreal regions) by default.

Data Retention: Customer Data is retained indefinitely until it is requested by the customer school to delete and destroy the data or upon termination of the agreement.

Storage Requirements: All Classified data is be stored by Google Cloud on secure, encrypted storage systems with appropriate access controls and monitoring mechanisms to prevent unauthorized access or data breaches. Employees are forbidden from storing any classified data on their personal machines.

Data Transfer: When transferring classified data internally or externally, secure channels and encryption protocols are used to safeguard data integrity and confidentiality. Classified data is not permitted to be transferred via email or other insecure method.

Data Backup Policy

Regular Backups: Scheduled backups will be performed daily to ensure that all critical data is backed up at predetermined intervals.

Offsite Storage: Backup data is stored by Google Cloud in secure, offsite locations to protect against onsite disasters, such as fire, flood, or theft.

Akindi Data & Security

Akindi Inc.

480 Adelaide St. W
Toronto, ON, M5V 1T2

www.akindi.com

Offsite storage facilities adhere to strict security standards and access controls.

Retention Period: Backups are retained for 6 month to ensure business continuity needs and data recovery objectives.

Regular Testing: Backup systems and procedures are tested regularly to verify the integrity and recoverability of backup data. Testing includes simulated recovery scenarios to ensure that data can be restored effectively in the event of a disaster.

Results of testing and exercises are documented, including observations, findings, lessons learned, and recommendations for improvement. Reports will be shared with relevant stakeholders, and corrective actions will be taken as necessary to address identified deficiencies.

Monitoring and Alerts: Monitoring systems are in place to track backup performance, identify any failures or anomalies, and generate alerts for prompt resolution.

Business Continuity and Disaster Recovery

IT Infrastructure Inventory: Akindi maintains an inventory of IT assets, systems, applications, and infrastructure components critical operations, including backup systems, data centers, servers, networking equipment, and cloud services.

Backup and Recovery: Akindi's hosting provider, Google Cloud has robust backup and recovery procedures to protect critical data and IT systems from loss or corruption. Database backups are performed daily, and backup copies are stored securely to facilitate recovery in the event of a disaster.

Emergency Notification: Akindi has established communication protocols and notification procedures for alerting employees, stakeholders, and

response teams in the event of a disruptive event. Contact lists and communication channels are maintained and updated regularly.

Akindi will notify relevant stakeholders as soon as is reasonable after the incident has been confirmed and not more than 4 hours after confirmation.

Coordination with External Partners: Akindi will coordinate with external partners, including third-party vendors, customers, and other stakeholders to facilitate the timely response, recovery, and restoration of critical operations following a disaster.

Akindi Inc.

480 Adelaide St. W
Toronto, ON, M5V 1T2

www.akindi.com

Akindi will work closely with its relevant service providers to perform a root cause analysis, and provide a report to affected customers detailing the cause of the incident, the data affected (if applicable), the steps taken to resolve the incident, and the proactive steps which will be taken to prevent similar incidents in the future.

Incident Review and Analysis: Akindi will conduct post-incident reviews and analysis of business continuity and disaster recovery events to assess the effectiveness of response efforts, identify areas for improvement, and implement corrective actions to enhance resilience and preparedness.

BC/DR Employee Training: Akindi provides training and awareness programs to employees, contractors, and stakeholders on business continuity and disaster recovery procedures, roles, and responsibilities. Training is conducted regularly to ensure preparedness and readiness for responding to emergencies.

Incident Response Plan

Definition of an 'incident': An incident is any situation which causes or could reasonably cause Student PII or grades to be revealed, leaked, or otherwise improperly exposed, students to receive incorrect grades, significant data

Akindi Data & Security

Akindi Inc.

480 Adelaide St. W
Toronto, ON, M5V 1T2

www.akindi.com

loss, a service interruption of more than 30 minutes, Akindi to fall out of compliance with contractual obligations.

Procedure following an incident: Akindi's response to an incident will depend on the nature and severity of the incident. In general, these principles will be followed:

1. In incidents involving PII exposure, data loss, or compliance, Akindi will notify the institutional point of contact of affected customers as soon as is reasonable after the incident has been confirmed (and not more than 4 hours after confirmation). Trust and transparency are of paramount importance to Akindi.

2. Incidents involving PII exposure, incorrect grading, data loss, and service interruptions are treated as high priority, and all reasonable Akindi resources will be devoted to them until they are resolved.

3. After the incident has been resolved, Akindi will work closely with its relevant service providers to perform a root cause analysis, and provide a report to affected customers detailing the cause of the incident, the data affected (if applicable), the steps taken to resolve the incident, and the proactive steps which will be taken to prevent similar incidents in the future. If applicable, Akindi will contact relevant law enforcement.

4. For ongoing incidents (ex, service interruptions or ongoing investigations into security incidents), Akindi will provide ongoing updates to affected customers, as appropriate to ensure the customer is kept abreast of the situation's status.

5. Akindi may chose not to notify customers of proactive steps it takes to resolve situations which could reasonably cause, but have not yet caused, an incident.

Akindi Data
& Security

Akindi Inc.

480 Adelaide St. W
Toronto, ON, M5V 1T2

www.akindi.com

Data Access Control Policy

Least Privilege: Access rights will be granted based on the principle of least privilege, ensuring that individuals have only the minimum level of access necessary to perform their job functions.

Need-to-Know Basis: Access to sensitive or confidential information will be restricted to authorized personnel who have a legitimate need-to-know based on their job responsibilities.

Segregation of Duties: Duties and responsibilities will be segregated to prevent conflicts of interest and reduce the risk of fraud or unauthorized activities. Critical tasks will require multiple individuals to complete, with no single person having full control over sensitive functions.

Access Control Measures

User Authentication: Strong authentication mechanisms, such as passwords, multi-factor authentication (MFA), to verify the identity of users accessing company systems and applications.

Access Controls: Role-based access control mechanisms is used to assign and manage user permissions based on their roles, responsibilities, and organizational hierarchy.

Access Requests: Access to information systems and data resources will be granted based on formal access requests submitted by authorized personnel and approved by technical lead and CEO.

Access Reviews: Regular access reviews are conducted to ensure that access rights remain appropriate and aligned with users' job functions. Any discrepancies or unauthorized access will be promptly addressed and remediated.

Akindi Data
& Security

Akindi Inc.

480 Adelaide St. W
Toronto, ON, M5V 1T2

www.akindi.com

Access Control Enforcement

Technical Controls: Access control mechanisms, such as firewalls, intrusion detection/prevention systems (IDS/IPS), endpoint security solution, and encryption, are implemented to enforce access policies and prevent unauthorized access attempts.

Remote Access Policies: Employees must use secure connections and Virtual Private Networks (VPNs) when remote accessing company systems and data.

Monitoring and Logging: Access activities will be monitored, logged, and audited to detect and investigate any suspicious or unauthorized access attempts. Logs will be retained according to established retention policies for forensic analysis and compliance purposes.

Access Policy Enforcement and Accountability

Employee Training: All employees will receive training on access control policies, procedures, and best practices to ensure awareness of their responsibilities and the importance of safeguarding company resources. Regular awareness programs, communications, and reminders will be conducted to reinforce access control principles, highlight security threats, and promote a culture of security awareness throughout the organization.

Responsibilities: It is the responsibility of all employees, contractors, and authorized users to adhere to this Access Control Policy and report any suspected violations or security incidents to the appropriate authorities.

Consequences of Violations: Violations of this policy may result in disciplinary action, including warnings, suspension of access privileges, termination of employment, or legal prosecution, depending on the severity and impact of the violation.