Security At DataRow

Security at DataRow

DataRow is a data warehouse management platform for Amazon Redshift, enabling people to develop their data faster and easier with cloud data integration tools. DataRow collects and tracks data for each required event during its lifecycle. The safe handling of this data is DataRow's top priority.

Security Framework

DataRow security is based on the ISO 27001 Information Security Standard and Cloud Security Alliance (CSA) Framework, which includes:

- Policies & procedures
- Personal security
- Physical security
- Operations security
- Communications security
- Supplier security
- Asset management
- Access management
- Security incident management
- Business continuity management
- Compliance
- Cryptography
- System development and maintenance

Security is the responsibility of all employees of DataRow, and each employee must complete regularly scheduled security training. The Chief of Security and Reliability Officer defines and implements the security program at DataRow. This program is reviewed with the executive team regularly to ensure the latest security measures are in place to keep customer data secure.

Policies & Procedures

To provide the basis of the information security framework, DataRow determines and performs a set of policies, procedures, standards, and guidelines. These documents are reviewed regularly by the executives and updated by the ISMS team as needed.

Personal Security

Security starts with the employee at DataRow. Every employee goes through a precise security process, which involves the following:

Background Checks

Information Security is inscribed at the recruitment stage, and background checks are done on all DataRow team member. Criminal and reference controls are performed before hire. The contract with each employee contains their responsibilities for information security as an employee of DataRow.

Training & Awareness

The ISMS team designed an information security training and awareness program which is in place so each employee can perform their functions efficiently and effectively.

We gave product and technology education featuring security-related topics to software developers in addition to technical security training. Employees report catastrophic events and vulnerabilities that may affect information security through management channels as quickly as possible.

Termination or change of employment

ISMS removes the terminated employee from all systems; disabling all access to any DataRow management systems, tools & platform the day the person formally leaves the company.

Employees who leave DataRow on their own or by termination are required to deliver all company assets, including but not limited to: computers, files, keys, and access cards on their last day.

Customer Data Protection

DataRow ISMS concentrates on protecting customer data from unauthorized access and implements the following controls:

Data Classification & Handling

DataRow classes customer data and practices the most proper way of handling, warehousing, recovering, and disposing of this data according to its classification. Customer data is classified at the top level.

Data Encryption in Transit and at Rest

DataRow adopts the best practice encryption algorithms for cryptographic controllers to assure the security of data and the environment that we store the data.

DataRow uses AWS KMS (AES-256 algorithm) or other industry-standards to encrypt data. TLS is used in transit as well. DataRow manages Encryption Keys by using AWS services coupled with industry-standard methods.

Applications use a layer between application business logic and database resources. This intermediate layer ensures that one customer is not able to access another customer's data. Data in databases are designed to be segmented for tenants.

Credit Card Information Security

DataRow uses Stripe as a third-party payment processing service. DataRow sends the credit card information directly to Stripe in an encrypted form. DataRow does not store, collect or process credit card information of customers. Stripe is PCI compliant, and our use of their service preserves that PCI compliance.

Systems & Communication Security

DataRow separates infrastructure, public-facing networks and private networks isolated from each other to protect customer data.

DataRow uses SSL protocol for transferring all customer data and applies IP restriction for accessing AWS.

DataRow protects public networks with multiple levels of firewall against global threats including DDOS spoofing & port scanning. The designated operators manage network systems with a specific business need. The development and maintenance section of this document describes how the changes are applied.

Wherever feasible, DataRow adopts serverless services provided by AWS by hardening security of these services.

Authentication & Authorization

The authorization of users in DataRow is set based on the least privilege to prevent the exposure of customer data due to unauthorized access.

ISMS audits, logs, and verifies access to the system. Management team reviews the access rights of users at least annually according to their job responsibilities at regular intervals by management.

DataRow restricts access to information, applications, and systems through username and password.

Logging

DataRow manages extensive logs specific to the application, operating system, and database layers. The responsible users and user groups monitor and review all log data.

DataRow protects log information against tampering and unauthorized access.

ISMS logs system administrator and system operator activities.

Protection from malware and malicious code

DataRow protects and monitors devices from malware, malicious and unsafe codes or applications by deploying a set of protection tools.

Change control

To prevent a breach of data, DataRow controls all changes in the production environment according to security requirements defined throughout this document. DataRow documents and approves all tests before deployment.

Development and maintenance

DataRow follows the Agile methodology for software development, which facilitates continuous development and deployment. DataRow releases features and bug fixes to production when completed.

DataRow handles new features and bug fixes as needed. The software development team uses a Continuous Delivery Model for the delivery of software, and a test-driven model for development. DataRow verifies all changes with an automated unit, integration, functional, performance, and security tests. Developers work collectively to examine changes.

DataRow complies with the OWASP Secure Web Application framework requirements, and tests for vulnerabilities regularly using vulnerability scanners.

Physical and environmental security

Data Center Security

We host DataRow entirely on Amazon Web Services (AWS). As a customer of DataRow, the security policies AWS provide to us are also applicable to you. The AWS data center operations comply with a set of standards and regulations including ISO 27001, SSAE 16, PCI Level 1, FISMA Moderate Sarbanes-Oxley (SOX), and HIPAA (at the server level).

For more information about Data Center Security of AWS, please refer to the AWS Security Whitepapers below.

https://d0.awsstatic.com/whitepapers/aws-security-whitepaper.pdf
https://aws.amazon.com/security
https://aws.amazon.com/compliance/shared-responsibility-model

Working in Secure Areas

There are surveillance cameras and security in place to monitor the buildings. Employees have ID badges for entering the office. The security team of the building escorts all visitors to the DataRow office.

Business Continuity and Disaster Recovery

DataRow is always running, reliable & scalable by design. Providing committed SLAs and ensuring business continuity is vital for us.

Availability Zone Failover

DataRow runs on two different data centers in a single region. DataRow continues being up and running, unless both availability zones have an outage at the same time

Region Failover

DataRow uses more than two hosting regions, which are located away from each other. In case of a regional breakdown in which all available zones have an outage, automated processes redirect customer data to the healthy region to avoid any downtime.

We monitor and test replication of each region at regular intervals.

Backup

DataRow backups the data and continuously replicates it to a different data center in a different region, and backups as encrypted files daily. Restore test of backups is done at regular intervals.

Monitoring & Security Incident Response

DataRow is a heavily-monitored SaaS platform. Our monitoring system can notify us of vulnerabilities, threats, and incidents, and there are automated fixes within our monitoring solution. The IT Team assesses the vulnerabilities, threats, and incidents and then performs remediation and moderation.

Supplier security

DataRow identifies and includes the information security requirements as part of the agreement or contract with the supplier or third-party to avoid any risk.

Compliance

DataRow complies with applicable legal, regulatory and contract requirements as well as industry best practices.

We store customer data for as long as it is needed to meet the operational needs of DataRow, together with contractual legal and regulatory requirements.

DataRow uses cryptographic controls in compliance with all applicable agreements, laws, and regulations.

We take regular technical compliance reviews, including penetration testing and IT health checks of all information systems to ensure continued compliance.