



Databricks Shared Responsibility Model

For the GCP classic data plane

Databricks
July 2023





Databricks Managed Services Shared Responsibility Model

Security and compliance are a shared responsibility between Databricks, the Databricks customer, and the cloud service provider (CSP) GCP. For their part, [GCP](#) has formalized their shared responsibility models.

Databricks Responsibilities

Databricks Platform and Services

- Secure the Databricks Control Plane
- Utilize industry standards to harden images and operating systems deployed under our control
- Maintain a public bug bounty program
- Maintain the Databricks Control Plane with updated code and images

Databricks Managed Resources

- Securely deploy and terminate Databricks managed systems
- Track security configurations against industry standard baselines for systems under Databricks control
- Deploy the latest applicable source code and system images upon launch of customer Data Plane hosts

Customer Responsibilities

Account and Workspace Management

- Manage account configurations, including account setup and administration, subscription management and cloud resources ([GCP](#))
- Workspace management, including workspace creation, update, and deletion, and workspace resource access ([GCP](#))

Cluster Policies

- Configure cluster management policies and personal compute policies ([GCP](#))

VM Instance Management

- Restart workspace cluster VMs to deploy the [latest patched images and code](#) in accordance with patch management policy ([GCP](#))

Cloud Responsibilities

Cloud Service Platform and Services

- Maintain security of the cloud service infrastructure
- Maintain a security management program that maintains reasonable security measures to protect customer data and services



Platform Security



IAM Security

Identity and Access Management

- Authenticate Databricks personnel using industry best practices
- Set employee privileges consistent with least privilege principles
- Limit access to systems processing customer data to employees with roles that warrant access
- Restricts access to customer content based on the principle of least privilege and segregation of duties
- Secure interactions with the customer-managed cloud account
- Secure storage and policy enforcement of secrets scope

Identity and Access Management

- Enable multi-factor authentication via your SSO provider
- Enable System for Cross-domain Identity Management (SCIM) integration with your identity provider ([GCP](#))

Identity, Service Principal and Access Management

- Manage users, groups, personal access tokens, and service principals ([GCP](#))
- Set Access Control Lists to restrict resource access (such as workspace objects, clusters, pools, jobs, tables) ([GCP](#))
- Secure management and use of secret scopes ([GCP](#))

Identity and Access Management

- Maintain access controls required to restrict access to authorized customer resources
- Restrict employee access to customer resources





Databricks Managed Services Shared Responsibility Model

Security and compliance are a shared responsibility between Databricks, the Databricks customer, and the cloud service provider (CSP) GCP. For their part, [GCP](#) has formalized their shared responsibility models.

Databricks Responsibilities

Databricks Managed Data

- Transmit customer content using TLS 1.2 or higher between the Customer and the Databricks Control Plane and the Databricks Control Plane and the Data Plane
- Encrypt customer data-at-rest within the Databricks Control Plane using AES-256 bit equivalent or higher
- Delete customer content contained within a customer workspace within thirty (30) days of the workspace cancellation

Secure Network Communications

- Separate the Databricks Control Plane from the Customer Data Plane and workspaces within the Databricks Data Plane using multiple layers of network security controls
- Deploy local firewalls or security groups within the Customer Data Plane to isolate clusters
- Enable secure defaults for network access controls and security groups within the Control Plane

Customer Responsibilities

Data Governance

- Enable [Unity Catalog](#) within your Databricks account
- Follow [data governance](#) best practices, as per your organization's requirements ([GCP](#))

Customer-managed Data

- Secure management of data infrastructure ([GCP](#)):
 - Secure connectivity to customer-managed resources
 - Secure service integration with Databricks ([GCP](#))

Cloud Network Security

- Configure Secure Cluster Connectivity ([GCP](#))
- Enable customer-managed networks ([GCP VPC](#))
- Configure Data Exfiltration Protection according to your organization's data protection policy (GCP)

IP Access Control Lists and Private Link

- Configure Databricks workspace IP access lists ([GCP](#))

Cloud Responsibilities

Cloud Service Managed Data

- Maintain encryption hardware and services
- Encrypt data in transit and at rest, where configured
- Maintain the confidentiality, integrity and availability of data stored on CSP services
- Enable Spark inter-cluster encryption (GCP)
- Enable Data Plane local disk encryption (GCP)

Secure Network Communications

- Secure the physical and logical security of cloud service networking
- Maintain secure network communications for cloud services, including APIs



Data Security



Network Security





Databricks Managed Services Shared Responsibility Model

Security and compliance are a shared responsibility between Databricks, the Databricks customer, and the cloud service provider (CSP) GCP. For their part, [GCP](#) has formalized their shared responsibility models.

Databricks Responsibilities

Security Monitoring

- Deploy security detection capabilities, including those provided natively by Cloud Service Providers
- Generate audit logs from customer's use of the platform services and retain them for at least one year
- Deliver audit logs from the customer's use of the platform services based on the customer's configuration (Premium subscriptions and above)
- Deploy a dedicated Detection engineering team that develops intrusion detection monitoring across its computing resources
- Employ an incident response framework to manage and minimize the effects of unplanned security events
- Notify customers of security breaches in accordance with data protection laws and customer agreements

Secure Code Execution

- Maintain availability and security of the job scheduler
- Secure delivery of customer code (such as notebooks, repos and models, queries) from the control plane to the data plane

Customer Responsibilities

Audit Log Configuration

- Configure Databricks [audit log delivery](#) to your cloud storage ([GCP](#))
- Configure [verbose](#) audit logs for your workspace(s) ([GCP](#))

Account and Workspace Security Monitoring

- Deploy account and workspace [security monitoring](#)
- Deploy cloud service security monitoring
- Investigate and respond to potential security incidents related to customer-managed features, services and resources

Application Security

- Perform security reviews of your code, libraries and jobs, such as notebooks ([GCP](#)), [Terraform](#), and third-party libraries ([GCP](#))

CI/CD Pipeline and Repo Integration

- Integrate Git with Databricks repos ([GCP](#))
- Manage CI/CD Pipeline integration with Databricks ([GCP](#))

Cloud Responsibilities

Security Monitoring

- Monitor for security violations of the underlying cloud service infrastructure and services
- Deliver audit logs for cloud service events based on customer configurations
- Employ an incident response framework
- Notify customer of a security breach for which that customer is impacted

Secure Code Execution

- Maintain secure cloud infrastructure



Security Monitoring



Code Execution / Jobs






Databricks Managed Services Shared Responsibility Model

Security and compliance are a shared responsibility between Databricks, the Databricks customer, and the cloud service provider (CSP) GCP. For their part, [GCP](#) has formalized their shared responsibility models.

Databricks Responsibilities

Customer Responsibilities

Cloud Responsibilities



Core Compliance

Standards and Compliance

- Maintain independent third-party audits, standards, and certifications that apply to all customer environments:
 - ISO 27001, 27017, 27018
 - SOC 2 Type II, SOC 1 Type II, SOC 3
- Provide tools and configurations that enable use of services in compliance with applicable laws (such as GDPR and CCPA)

** Additional compliance standards covered later, such as HIPAA, FedRAMP, PCI*

Maintain Adherence to Relevant Compliance and Standards:

- When using Databricks to process sensitive data such as PII, adhere to relevant privacy regulations such as the GDPR and CCPA
- Review your compliance needs and add optional compliance service offering where required (such as for FedRAMP, PCI-DSS, HIPAA)
- Comply with applicable laws when using Databricks, including by implementing any required configurations in accordance with Databricks documentation

Standards and Compliance

- Maintain independent third party audit, standards and certifications
- Maintain relevant independent third-party audits, standards, and certifications
- Maintain relevant compliant services



Disaster Recovery

Maintain Disaster Recovery Capabilities* For:

- Review Business Continuity and Disaster Recovery plans annually
- Conduct Business Continuity and Disaster Recovery drills annually
- Conduct periodic backups of the Databricks Control Plane*

Data Backups

- Backup of your organization's [account and workspace](#)
- Set [Recovery Point Objectives](#) (RPO) and [Recovery Time Objectives](#) (RTO) using best practices ([GCP](#))

Disaster Recovery capabilities

- Cloud service capacity
- Review Business Continuity and Disaster Recovery plans annually
- Conduct Business Continuity and Disaster Recovery drills annually



Security Best Practices

Employ Security Best Practices

- Periodically review cryptographic standards to select and update technologies and ciphers in accordance with assessed risk and market acceptance of new standards
- Maintain a vulnerability management program that follows industry best practices
- Conduct third-party penetration tests at least annually
- Employ an in-house offensive security team

Multi-region Workspace Deployment

- Adopt Databricks security best practices based on the organization's cybersecurity requirements ([GCP](#))
- Follow security best practices for the customer's cloud environment ([GCP](#))

Employ Security Best Practices

- Review cryptographic standards
- Regularly run authenticated vulnerability scans
- Address vulnerabilities within SLAs
- Conduct third-party penetration tests