



# Databricks Shared Responsibility Model

*For the AWS classic data plane*

---

**Databricks**  
February 2025





# Databricks Managed Services Shared Responsibility Model

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

## Databricks Responsibilities

### Databricks Platform and Services

- Secure the Databricks Control Plane
- Utilize industry standards to protect Databricks infrastructure
- Publish CIS level 1 hardened control plane and data plane images
- 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

### 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

## Customer Responsibilities

### Account and Workspace Management

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

### Cluster Policies

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

### Identity and Access Management

- Setup Unified Login access controls for Databricks account and workspace(s) ([AWS](#))
- Enable multi-factor authentication via your SSO provider
- Enable System for Cross-domain Identity Management (SCIM) integration with your identity provider ([AWS](#))

### Identity, Service Principal and Access Management

- Manage users, groups, personal access tokens, and service principals ([AWS](#))
- Set Access Control Lists to restrict resource access (such as workspace objects, clusters, pools, jobs, tables) ([AWS](#))
- Use least-privilege principles for cross-account IAM roles ([AWS](#))
- Secure management and use of secret scopes ([AWS](#))

## 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

### Identity and Access Management

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



Platform Security



IAM 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) AWS. For their part, [AWS](#) has formalized their shared responsibility model.

## 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



Data Security

### 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



Network Security

## Customer Responsibilities

### Data Governance

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

### Customer-managed Data

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

### Customer-managed Encryption Keys

- Deploy customer-managed encryption keys (CMK) ([AWS](#))
  - Enable CMK for managed services
  - Enable CMK for workspace storage

### Cloud Network Security

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

### IP Access Control Lists and Private Link

- Configure Databricks workspace IP access lists ([AWS](#))
- Configure Private Link access for Users → Control Plane and Control Plane → Data Plane connections ([AWS](#))

## 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 ([AWS Nitro](#) that [support in-transit encryption](#))
- Enable Data Plane local disk encryption ([AWS Nitro](#) or [NVMe](#))

### Secure Network Communications

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





# Databricks Managed Services Shared Responsibility Model

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

## Databricks Responsibilities

## Customer Responsibilities

## Cloud Responsibilities



### Security Monitoring

#### 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 (Premium subscription +)
- Deliver audit logs from the customer's use of the platform services based on the customer's configuration (Premium subscriptions +)
- 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

#### Audit Log Configuration

- Enable Databrick System Tables for security and performance monitoring ([AWS](#))
- Alternatively, configure Databricks audit log delivery to your cloud storage ([AWS](#))
- Configure verbose audit logs for your workspace(s) ([AWS](#))

#### 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

#### 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



### Code Execution / Jobs

#### 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

#### Application Security

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

#### CI/CD Pipeline and Repo Integration

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

#### Secure Code Execution

- Maintain secure cloud infrastructure



### Vulnerability & Patch Management

#### Patching and Vulnerability Management

- Maintain a vulnerability management program that follows industry best practices, performs daily and weekly authenticated vulnerability scans against Databricks infrastructure and services
- Regularly release updated data plane images with patches that meet our [Security Addendum patch SLAs](#)

#### Patching and Vulnerability Management

- Restart workspace cluster VMs as needed to deploy the latest patched images and code in accordance with patch management policy ([AWS](#))
- Optionally, configure *Automatic cluster update* to automate cluster restarts during maintenance windows ([AWS](#))

#### Scan and Patch Cloud Infrastructure

- Scan and patch the cloud's infrastructure, firmware and software, etc. it manages, such as networking, servers, and virtualization





# Databricks Managed Services Shared Responsibility Model

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

## 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
- Enable compliant workflows supported by [Databricks](#)

*\* 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 and regulations

### Standards and Compliance

- Maintain independent third party audit, standards and certifications
- Maintain 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 ([AWS](#))

### 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
- 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 ([AWS](#))
- Follow security best practices for the customer's cloud environment ([AWS](#))

### Employ Security Best Practices

- Follow industry best practices
- Review cryptographic standards
- Conduct third-party penetration tests



# AWS Serverless Shared Responsibility Model







# Databricks Managed Serverless Services Shared Responsibility Model

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

## Databricks Responsibilities

### Databricks Platform and Services

- Secure the Databricks Control Plane
- Utilize industry standards to protect Databricks infrastructure
- Deploy CIS level 1 hardened control plane and data plane images
- 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 Compute Plane hosts

## Customer Responsibilities

### Account and Workspace Management

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

## 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
- Restrict 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

- Setup Unified Login access controls for Databricks account and workspace(s) ([AWS](#))
- Enable multifactor authentication via your SSO provider
- Enable SCIM integration with your identity provider ([AWS](#))

### Identity, Service Principal and Access Management

- Manage users, groups, personal access tokens, and service principals ([AWS](#))
- Set Access Control Lists to restrict access (such as workspace objects, serverless endpoints, jobs, tables) ([AWS](#))
- Use least-privilege principles for cross-account IAM roles ([AWS](#))
- Secure management and use of secret scopes ([AWS](#))

### Identity and Access Management

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





# Databricks Managed Serverless Services Shared Responsibility Model

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

## Databricks Responsibilities

### Databricks Managed Data

- Encrypt Databricks communications between the Databricks Control Plane and the customer workspace using TLS 1.2 or higher
- 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
- Enable local disk encryption for serverless drives



Data Security

## Customer Responsibilities

### Data Governance

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

### Customer-Managed Data

- Secure management of data infrastructure ([AWS](#)):
  - Secure connectivity to customer-managed resources

### Customer-Managed Encryption Keys

- Enable customer-managed encryption keys (CMK), where required ([AWS](#))
  - Enable CMK for managed services
  - Enable CMK for workspace storage

## 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 Compute Plane local disk encryption ([AWS Nitro](#) or [NVMe](#))

### Cloud Network Security

- Configure secure connectivity from the control plane to the Serverless Compute Plane

### Secure Network Communications

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



Network Security

### IP Access Control Lists and Private Link

- Configure Serverless Egress Controls (SEG) ([AWS](#))
- Configure Databricks workspace IP access lists ([AWS](#))
- Configure Private Link for user access to the Control Plane ([AWS](#))
- Configure Data Exfiltration Protection according to your organization's data protection policy ([AWS](#))

### Secure Network Communications

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







# Databricks Managed Serverless Services Shared Responsibility Model

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

## Databricks Responsibilities

## Customer Responsibilities

## Cloud Responsibilities



Security Monitoring

### 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 (Premium subscription+)
- Deliver audit logs from the customer's use of the platform services based on customer configurations (Premium subscription+)
- 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
- Deploy security monitoring for tenant isolation in the serverless compute plane

### Audit Log Configuration

- Enable Databrick System Tables for security and performance monitoring ([AWS](#))
- Alternatively, configure Databricks audit log delivery to your cloud storage ([AWS](#))
- Configure verbose audit logs for your workspace(s) ([AWS](#))

### Account and Workspace Security Monitoring

- Deploy account, workspace security monitoring
- Investigate and respond to potential security incidents in your Databricks account and workspace(s) for systems under your control

### 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



Code Execution / Jobs

### 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 compute plane

### Application Security

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

### CI/CD Pipeline and Repo Integration

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

### Secure Code Execution

- Maintain secure cloud infrastructure



Vulnerability & Patch Management

### Patching and Vulnerability Management

- Maintain a vulnerability management program that follows industry best practices, performs daily and weekly authenticated vulnerability scans against Databricks serverless infrastructure and services
- Regularly release updated serverless images with patches that meet our [Security Addendum patch SLAs](#)
- Restart active clusters after seven (7) days

### Restart Clusters to Deploy the Latest Patches

- Restart active serverless clusters to deploy instances with the latest patches (if required before the cluster is active for seven days) ([AWS](#))

### Scan

- Scan and patch the cloud's infrastructure, firmware and software, etc. it manages, such as networking, servers, and virtualization



# Databricks Managed Serverless Services Shared Responsibility Model

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

## Databricks Responsibilities

## Customer Responsibilities

## Cloud Responsibilities



### Core Compliance

#### Standards and Compliance

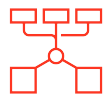
- Maintain independent third-party audits, standards, and certifications that apply to all customer environments:
  - ISO 27001, 27017, 27018
  - SOC 2 Type II, SOC 1 Type II, SOC 3
- Enable compliant workflows supported by [Databricks](#)

#### Maintain adherence to relevant compliance and standards:

- Comply with applicable laws and regulations
- When using Databricks to process sensitive data such as PII, adhere to relevant privacy regulations such as the GDPR and CCPA

#### Standards and Compliance

- Maintain independent third party audit, standards and certifications
- Enable compliant workflows supported by the cloud vendor



### 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 ([AWS](#))

#### 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
- 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 cyber risk appetite ([AWS](#))
- Follow security best practices for the customer's cloud environment based on the organization's cyber risk appetite ([AWS](#))

#### Employ security best practices

- Follow industry best practices
- Review cryptographic standards
- Conduct third-party penetration tests





# Databricks ESM/CSP Shared Responsibility Model



# Databricks Managed Services Shared Responsibility Model

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

## Databricks Responsibilities

## Customer Responsibilities

## Cloud Responsibilities



### Enhanced Security Monitoring

#### Databricks Enhanced Security Monitoring (ESM) Responsibilities

- Deploy ESM instances with enhanced CIS Level 1 hardening
- Deploy antivirus, behavior-based malware and file integrity monitoring
- Provide vulnerability reports of the host OS upon request
- Leverage FIPS 140-2 Level 1 encryption services where available

#### Customer Enhanced Security Monitoring Responsibilities

- Enable Enhanced Security Monitoring on your workspace(s) ([AWS](#))
- Monitor enhanced event logs for security incidents ([AWS](#))
- Restart relevant clusters to deploy as ESM instances.
- Provide the destination Email for vulnerability reports delivery

#### CSP ESM Responsibilities

- Maintain security of the cloud service infrastructure



### Compliance Security Profile

#### Databricks Compliance Security Profile (CSP) Responsibilities

- Enable ESM security enhancements (listed above)
- Enforcement of AWS Nitro instances on CSP workspace(s)
- Automatically restart clusters active past the maintenance window to deploy the latest patches

#### Customer Compliance Security Responsibilities

- Prepare workspace(s) for the compliance security profile ([AWS](#))
- Enable the Compliance Security Profile on relevant workspace(s) ([AWS](#))

#### CSP Compliance Responsibilities

- Maintain security of the cloud service infrastructure



### HIPAA, PCI, DoD and FedRAMP

#### Databricks HIPAA, PCI and FedRAMP Responsibilities

- Complete annual HIPAA, PCI-DSS, FedRAMP audits ([region and cloud specific](#))
- Provide HIPAA, PCI and FedRAMP (Moderate on AWS) compliant internal services
- Enforce Enterprise Security Monitoring and Compliance Security Profile features

#### Customer HIPAA, PCI, FedRAMP Responsibilities

- Enable Compliance Security Profile on relevant workspaces ([AWS](#))
- Use only supported preview features ([PCI](#), [HIPAA](#))
- Comply with compliance-specific prerequisites:
  - Detailed docs: [AWS: HIPAA, PCI, FedRAMP](#)
  - Obtain entitlement to process regulated data on Databricks
  - Comply with the PCI Shared Responsibility Model
  - Follow FedRAMP PMO documentation requirements ([FedRAMP](#))

#### CSP HIPAA, PCI and FedRAMP Responsibilities

- Complete annual HIPAA, PCI-DSS, FedRAMP audits



### GDPR/CCPA

#### Databricks GDPR/CCPA Service Responsibilities

- Provide services that are GDPR/CCPA compliant (subject to customer responsibilities)

#### Customer GDPR/CCPA Service Responsibilities

- Maintain GDPR/CCPA compliant usage of Databricks services

#### CSP GDPR/CCPA Responsibilities

- Provide service that are GDPR/CCPA compliant

