AWS Cloud Compliance Policy

Document ID: AWS-POL-2025-001
Effective Date: January 15, 2025
Approved By: CISO
Applies To: All engineering, DevOps, and data teams using AWS services.

---

1. Purpose

This policy defines mandatory compliance requirements for managing workloads on AWS. It ensures adherence to industry regulations (ISO 27001, SOC 2, PCI DSS, HIPAA where applicable) and AWS security best practices. The policy establishes comprehensive standards for resource tagging, password rotation, and security controls across all AWS services.

---

2. Scope

This policy applies to:

- All AWS accounts (Production, Development, Sandbox, DR)
- All AWS services used within the organization
- All employees, contractors, and third-party vendors with AWS access
- All resources created or managed within AWS environments
- Third-party integrations and external services connected to AWS

---

3. Policy Requirements

3.1 Identity and Access Management (IAM)

- MFA: Mandatory for all IAM users and AWS SSO accounts.
- Principle of Least Privilege: Permissions must grant only the access required.
- Role Reviews: IAM roles and policies must be reviewed every 90 days.
- Account Hygiene: Inactive IAM users must be deactivated within 7 days.
- Password Policy Requirements:

    - Minimum password length: 14 characters
    - Must contain uppercase, lowercase, numbers, and special characters
    - Password expiration: 90 days
    - Password history: Last 24 passwords cannot be reused
    - Account lockout after 5 failed attempts
- Access Key Rotation:
    - IAM user access keys must be rotated every 90 days
    - Service account keys must be rotated every 180 days
    - Unused access keys must be deactivated after 30 days
- Root Account Protection:
    - Root account must have MFA enabled
    - Root account access keys must be deleted
    - Root account usage must be monitored and alerted

3.2 Data Protection

- Encryption:
    - All S3 buckets must enforce server-side encryption (AES-256 or AWS KMS).
    - RDS, EBS, and backups must be encrypted at rest.
    - DynamoDB tables must use encryption at rest
    - EFS file systems must be encrypted
    - Secrets Manager and Parameter Store must use KMS encryption
- Data in Transit: All public endpoints must enforce TLS 1.2+.
- Sensitive Data: Storing PII/PCI/HIPAA data in AWS requires written approval from the Security Team.
- Data Classification Requirements:
    - All data must be classified as: Public, Internal, Confidential, or Restricted
    - Restricted data requires additional encryption and access controls
    - Data retention policies must align with regulatory requirements

3.3 Logging and Monitoring

- CloudTrail: Must be enabled in all AWS accounts and all regions.
- Centralized Logging: Logs must be shipped to a central S3 bucket with retention of at least 7 years.
- Monitoring: CloudWatch Alarms must be configured for critical events:
    - Failed log delivery
    - IAM policy changes
    - Unauthorized API calls
    - Root account usage

    - Security group changes
    - Network ACL changes
    - Route table modifications
- Security Services:
    - GuardDuty must be enabled in all accounts
    - Security Hub must be enabled for compliance monitoring
    - Inspector must scan EC2 instances monthly
    - Config must track configuration changes
    - Macie must monitor S3 buckets containing sensitive data
- VPC Flow Logs: Must be enabled for all VPCs with 90-day retention

3.4 Infrastructure Security

- Network Controls:
    - Security Groups must follow least privilege principles
    - Public access to databases is prohibited
    - Default security groups must not be used
    - Unnecessary ports must be closed
    - NACL rules must be documented
- VPC Requirements:
    - Production VPCs must use private subnets for compute resources
    - Internet Gateway access must be restricted and monitored
    - NAT Gateways must be used for outbound internet access
    - VPC Peering must be approved by Network Team
- Patch Management:
    - Critical patches must be applied within 7 days
    - All other patches within 30 days of release
    - Patch compliance must be tracked via Systems Manager
- Instance Security:
    - EC2 instances must use approved AMIs
    - Instance metadata service v2 (IMDSv2) must be enforced
    - Public IP addresses require approval
    - SSH/RDP access must use Session Manager or bastion hosts

3.5 Resource Tagging Requirements

All AWS resources must include the following mandatory tags:

- Environment: Production, Staging, Development, DR, Sandbox
- Owner: Email address of resource owner or team
- CostCenter: Financial cost center code (format: CC-XXXXX)

- Project: Project or application identifier
- DataClassification: Public, Internal, Confidential, Restricted
- ComplianceScope: HIPAA, PCI-DSS, SOC2, GDPR, ISO27001, None
- CreatedDate: Resource creation date (YYYY-MM-DD)
- LastReviewedDate: Last compliance review date (YYYY-MM-DD)
- BackupRequired: true or false
- MaintenanceWindow: Preferred maintenance schedule (e.g., SAT:03:00-SAT:05:00)
- Department: Organizational department
- ExpirationDate: For temporary resources (YYYY-MM-DD)

Service-Specific Additional Tags:

- EC2 Instances:
  - OperatingSystem
  - PatchGroup
  - AutoShutdown
  - InstanceRole
  - MonitoringLevel
- RDS Databases:
  - DatabaseEngine
  - BackupRetentionDays
  - MultiAZ
  - EncryptionEnabled
- S3 Buckets:
  - BucketPurpose
  - VersioningEnabled
  - LifecyclePolicy
  - PublicAccessBlock
- Lambda Functions:
  - Runtime
  - MemorySize
  - Timeout
  - TracingConfig

3.6 Password and Secret Rotation

Rotation Schedule Requirements:

Credential Type	Maximum Age	Rotation Frequency	Grace Period	Notification

AWS Root Account	365 days	Quarterly (90 days)	7 days	14 days before
IAM User Passwords	90 days	Every 90 days	7 days	14 days before
IAM Access Keys	90 days	Every 90 days	0 days	7 days before
Database Master Passwords	30 days	Every 30 days	3 days	7 days before
Application Passwords	60 days	Every 60 days	3 days	7 days before
Service Account Keys	180 days	Every 180 days	14 days	30 days before
API Keys	365 days	Annually	30 days	60 days before
SSL/TLS Certificates	Before expiry	30 days before	7 days	60 days before

AWS Secrets Manager Requirements:

- All database credentials must be stored in Secrets Manager
- Automatic rotation must be enabled for supported secret types
- Custom rotation Lambda functions required for non-standard secrets
- Failed rotations must trigger immediate alerts

3.7 Backup and Disaster Recovery

- Backup Requirements:
    - All production databases must have automated backups
    - Backup retention: 30 days minimum for production
    - Cross-region backup for critical systems
    - Backup encryption is mandatory
    - Backup testing must occur quarterly
- Disaster Recovery:
    - RPO (Recovery Point Objective): 4 hours for critical systems
    - RTO (Recovery Time Objective): 2 hours for critical systems

    - DR drills must be conducted quarterly
    - DR runbooks must be maintained and tested

3.8 Container and Serverless Security

- ECS/EKS Requirements:
    - Container images must be scanned for vulnerabilities
    - Only approved base images may be used
    - Secrets must not be embedded in images
    - Network policies must restrict pod-to-pod communication
- Lambda Requirements:
    - Functions must use least privilege execution roles
    - Environment variables must not contain secrets
    - Reserved concurrent executions for critical functions
    - Dead letter queues for failed invocations

3.9 Database Security

- RDS/Aurora Requirements:
    - Deletion protection enabled for production databases
    - Performance Insights enabled with 7-day retention
    - Automated backups with point-in-time recovery
    - Read replicas must be encrypted
    - Database activity streams for audit logging
- DynamoDB Requirements:
    - Point-in-time recovery enabled
    - Contributor Insights for access patterns
    - Auto-scaling configured for production tables
    - Global tables for multi-region applications

3.10 Storage Security

- S3 Requirements:
    - Bucket policies must deny unencrypted uploads
    - Versioning enabled for production buckets
    - MFA delete for critical buckets
    - Object Lock for compliance data
    - Lifecycle policies for cost optimization
    - Access logging enabled
    - Public access blocked by default
- EBS Requirements:
    - Snapshots must be encrypted

    - Snapshot lifecycle policies configured
    - Volume deletion protection for production

3.11 Compliance Framework Alignment

The team must ensure AWS usage complies with:

- ISO 27001:
    - Access control and authentication
    - Encryption and key management
    - Logging and monitoring
    - Incident response procedures
    - Risk assessment and treatment
- SOC 2 (Security, Availability, Confidentiality):
    - Change management controls
    - Logical access controls
    - System monitoring
    - Risk mitigation
- PCI DSS (if handling cardholder data):
    - Network segmentation
    - Strong cryptography
    - Access logging and monitoring
    - Quarterly vulnerability scans
    - Annual penetration testing
- HIPAA (if handling health data):
    - PHI encryption at rest and in transit
    - Access tracking and audit controls
    - Business Associate Agreements (BAAs)
    - Minimum necessary access
- GDPR (if handling EU personal data):
    - Data residency controls
    - Right to erasure implementation
    - Data processing agreements
    - Privacy by design

---

4. Roles and Responsibilities

- Engineering Team:
    - Ensure daily compliance with this policy

    - Implement required tags on all resources
    - Rotate credentials per schedule
    - Report security incidents immediately
- DevOps Team:
    - Implement automation for monitoring and enforcement
    - Maintain CI/CD security controls
    - Configure backup and DR systems
    - Deploy security monitoring tools
- Security Team:
    - Review compliance every quarter
    - Audit IAM and logging practices
    - Investigate security incidents
    - Maintain security tooling
    - Conduct security assessments
- Managers:
    - Ensure all team members are trained on compliance requirements
    - Approve access requests
    - Review team compliance metrics
    - Escalate violations appropriately
- Cloud Architecture Team:
    - Define secure architecture patterns
    - Review and approve AWS service usage
    - Maintain reference architectures
    - Provide technical guidance

---

5. Enforcement

- Violations:
    - First violation: Written warning and remediation plan
    - Second violation: Suspension of AWS access pending training
    - Third violation: Disciplinary action up to termination
- **Non-compliance incidents must be reported within 24 hours to the Security Team
- Automated Enforcement:
    - Non-compliant resources will be automatically tagged for review
    - Resources missing critical tags will be terminated after 7 days
    - Expired credentials will be automatically deactivated
    - Non-encrypted resources will be blocked from creation
- Exceptions:

    - Must be approved by CISO and documented
    - Valid for maximum 90 days
    - Must include compensating controls
    - Subject to additional monitoring

---

6. Compliance Monitoring and Reporting

- Continuous Monitoring:
    - AWS Config rules evaluate compliance real-time
    - Security Hub provides compliance scores
    - CloudWatch dashboards track metrics
    - Automated alerts for violations
- Reporting Requirements:
    - Weekly compliance summary to management
    - Monthly detailed compliance report
    - Quarterly executive dashboard
    - Annual compliance attestation
- Key Performance Indicators (KPIs):
    - Tag compliance rate (target: >95%)
    - Password rotation compliance (target: 100%)
    - Patch compliance rate (target: >98%)
    - Encryption coverage (target: 100%)
    - Security finding resolution time (target: <48 hours)

---

7. Training and Awareness

- Required Training:
    - AWS Security Fundamentals (annually)
    - Compliance policy training (onboarding + annually)
    - Incident response procedures (bi-annually)
    - Service-specific security training (as needed)
- Certification Requirements:
    - Cloud architects must maintain AWS certifications
    - Security team must have security specialty certification
    - DevOps team must complete AWS DevOps certification

---

8. Incident Response

- Incident Classification:
  - Critical: Data breach, account compromise, service outage
  - High: Policy violations, failed security controls
  - Medium: Non-critical misconfigurations
  - Low: Minor compliance gaps
- Response Times:
  - Critical: Immediate response, resolution within 4 hours
  - High: Response within 1 hour, resolution within 24 hours
  - Medium: Response within 4 hours, resolution within 3 days
  - Low: Response within 1 day, resolution within 7 days
- Incident Response Team:
  - Security Team Lead
  - Cloud Architecture representative
  - DevOps on-call engineer
  - Affected service owner
  - Legal/Compliance (if required)

---

9. Policy Exceptions

- Exception Request Process:
  - Submit written request with business justification
  - Include risk assessment and mitigation plan
  - Obtain manager approval
  - Security team review and recommendation
  - CISO final approval
- Exception Requirements:
  - Must not violate regulatory requirements
  - Must include compensating controls
  - Must have defined expiration date
  - Subject to enhanced monitoring
  - Reviewed monthly

---

10. Review and Updates

- This policy will be reviewed annually or upon:
    - Significant changes in AWS services
    - New compliance regulations
    - Major security incidents
    - Organizational changes
- Review Committee:
    - CISO (Chair)
    - Cloud Architecture Lead
    - DevOps Manager
    - Security Team Lead
    - Compliance Officer
    - Engineering Manager
- Update Process:
    - Proposed changes reviewed by committee
    - Impact assessment conducted
    - Stakeholder consultation
    - CISO approval required
    - 30-day notice before implementation

---

11. References and Related Documents

- AWS Well-Architected Framework
- CIS AWS Foundations Benchmark
- NIST Cybersecurity Framework
- Organization Information Security Policy
- Incident Response Plan
- Business Continuity Plan
- Data Classification Policy
- Third-Party Risk Management Policy

---

12. Appendices

Appendix A: Approved AWS Services

Compute: EC2, Lambda, ECS, EKS, Batch, Lightsail
Storage: S3, EBS, EFS, FSx, Storage Gateway

Database: RDS, DynamoDB, Aurora, DocumentDB, Neptune
Networking: VPC, CloudFront, Route 53, API Gateway, Transit Gateway
Security: IAM, KMS, Secrets Manager, Certificate Manager, WAF
Monitoring: CloudWatch, CloudTrail, Config, Security Hub, GuardDuty
Developer Tools: CodeCommit, CodeBuild, CodeDeploy, CodePipeline

Appendix B: Prohibited Practices

- Hardcoding credentials in code
- Using default security groups
- Exposing databases to internet
- Disabling CloudTrail logging
- Sharing IAM user credentials
- Using root account for daily operations
- Storing unencrypted sensitive data
- Ignoring security alerts
- Bypassing change management
- Creating public S3 buckets without approval

Appendix C: Compliance Checklist

Daily Tasks:

- Review CloudWatch alarms
- Check GuardDuty findings
- Monitor cost anomalies
- Verify backup completion

Weekly Tasks:

- Review IAM credential report
- Check Config compliance
- Audit new resources for tags
- Review security group changes

Monthly Tasks:

- Rotate passwords due for rotation
- Review and update documentation
- Conduct access review
- Patch compliance check
- Cost optimization review

Quarterly Tasks:

- Full compliance audit
- DR drill execution
- Security assessment
- Policy review
- Training completion check

Appendix D: Contact Information

Security Team: security@company.com | On-call: +1-xxx-xxx-xxxx
Cloud Team: cloudops@company.com | On-call: +1-xxx-xxx-xxxx
Compliance: compliance@company.com
Incident Response Hotline: +1-xxx-xxx-XXXX (24/7)

Document Revision History

Version	Date	Author	Changes
1.0	2025-01-15	Security Team	Initial policy release

Keywords for Search: AWS, Compliance, Security, Policy, IAM, Encryption, Tagging, Password Rotation, Monitoring, CloudTrail, GuardDuty, Config, Backup, Disaster Recovery, HIPAA, PCI-DSS, SOC2, GDPR, ISO27001, Incident Response, Training, Audit