Security & Compliance

This page provides an overview of the security model used by **Sandbox Studio**. It explains how the solution is deployed, the controls in place, and how it aligns with enterprise security, compliance, and governance requirements.

Deployment Model

- **Customer-owned deployment** – Sandbox Studio is deployed into your own **AWS Organisation or Landing Zone**. It is not SaaS.
- **Full control** – You retain complete ownership of AWS accounts, configurations, and network boundaries.
- **Account isolation** – Sandbox accounts are provisioned into dedicated **Organisational Units (OUs)** with **Service Control Policies (SCPs)** applied to enforce guardrails.

Data Protection

- **No production data ingestion** – Sandbox Studio does not ingest, store, or process production workloads unless specifically configured to do so.
- **Local metadata** – Configuration data, logs, and monitoring outputs remain within your AWS accounts unless explicitly shared.
- **Encryption standards**:
  - **In transit** – All communication uses TLS 1.2 or higher.
  - **At rest** – All persistent data is encrypted with AWS KMS (customer-managed where appropriate).
- **Credential handling** – No AWS credentials are stored outside your environment.

Identity & Access Management

IAM Roles

- Multiple **IAM roles** are deployed to run Sandbox Studio and discover resources within AWS accounts.
- Roles follow **least privilege principles**, granting only the minimal permissions required for each function.
- Separation of duties is enforced across deployment, lifecycle automation, and monitoring components.

IAM Identity Center & SAML

- **AWS IAM Identity Center** (formerly AWS SSO) provides **centralised authentication**.

- Sandbox Studio integrates with **SAML 2.0 identity providers** (e.g., Okta, Microsoft Entra ID) for seamless single sign-on.
- Users sign into the Sandbox Studio web UI with **existing corporate credentials**, eliminating the need for local passwords.

Role-based Access

- Access levels are defined by **permission sets**:
  - **End users** – Request and operate sandbox accounts.
  - **Managers** – Approve requests, define templates, and oversee usage.
  - **Administrators** – Configure global settings, guardrails, and integrations.
- **SCP enforcement** prevents privilege escalation, service misuse, or bypassing of governance controls.

Network Security

Sandbox Studio backend services run inside a **dedicated VPC** with a layered subnet model to enforce isolation.

- **Three subnet tiers**:
  - **Public subnet** – Only for CloudFront distribution and API Gateway.
  - **Private application subnets** – Run AWS Lambda functions with **controlled outbound-only egress** for required API calls.
  - **Private database subnets** – Host PostgreSQL RDS, with **no inbound or outbound internet access**.
- **No direct internet exposure** – Backend compute and storage remain fully private.
- **AWS WAF protection** – A **regional WAF ACL** secures API Gateway endpoints using four AWS managed rule groups and two custom rules.
- **Separation of duties** – Network boundaries ensure web entry points, compute, and data tiers are isolated.

Core Security Services

AWS Key Management Service (KMS)

- Sandbox Studio creates **four Customer Managed Keys (CMKs)**, one per stack (AccountPool, IDC, Data, Compute).
- Each CMK encrypts AWS resources such as:
  - CloudWatch Logs
  - Amazon SQS queues
  - EventBridge event buses
  - AWS Secrets Manager secrets
  - AWS CodeBuild projects
  - Amazon RDS database
- CMKs follow **separation of concerns**, limiting key scope and permissions per stack.

AWS WAF

- Web Application Firewall (WAF) protects **API Gateway endpoints**.
- Rules include managed protections (e.g., SQLi, XSS, bot control) and two custom allowlists.
- Default behaviour blocks any request failing rule evaluation.

Amazon CloudFront

- Serves the Sandbox Studio web UI hosted in **Amazon S3**.
- Configured with **TLS 1.2+** for all sessions.
- Adds **HTTP security headers** to viewer responses.
- For stricter TLS enforcement, a custom certificate can be applied to require TLS 1.2 or TLS 1.3.

Amazon RDS

- All user data stored in **Amazon RDS** (Relational Database Service) is encrypted at rest with **AWS KMS CMKs**.

AWS Lambda

- All backend logic runs on **serverless Lambda functions**.
- Each function uses the **most recent stable runtime**.
- **No secrets are logged**, and IAM roles are isolated per function.
- Functions operate with **least-privilege permissions** and scoped network access.

Lifecycle Management

- **Pre-configured templates** – Sandboxes are provisioned with security guardrails and governance baked in.
- **Automated teardown** – On expiry, AWS Nuke ensures accounts are cleaned and reset before reuse.
- **Flexible expiry options** – Accounts may expire based on **time** or **budget thresholds**. Logs are retained for audit purposes.

Logging, Monitoring & Governance

- **AWS-native monitoring** is fully supported. Customers are able to use the following native AWS services and are encouraged to do so to increase their security posture:
  - **AWS CloudTrail** – Comprehensive audit logging.
  - **AWS Config** – Compliance and drift detection.
  - **Amazon GuardDuty** – Continuous threat detection.
  - **Amazon CloudWatch** – Metrics, alarms, and application insights.
- **Governance enforcement** – SCPs and automation to prevent insecure patterns (e.g. public S3 buckets).

Compliance Alignment

While Sandbox Studio itself is not independently certified, it is **built entirely on AWS services that hold stringent compliance certifications**. This means Sandbox Studio inherits the **trusted compliance foundation** of AWS.

Key AWS Certifications in Scope

AWS services underpinning Sandbox Studio have been audited against major frameworks, including:

- **SOC 1, SOC 2, SOC 3**
- **PCI DSS**
- **HIPAA / HITECH**
- **ISO 27001, ISO 27017, ISO 27018**
- **FedRAMP**
- **GDPR**
- **FIPS 140-3** (for AWS KMS)

Compliance Certifications for Core Services

Service	Certifications
Amazon CloudFront	SOC 1, SOC 2, SOC 3, PCI DSS, HIPAA, ISO 27001/17/18, FedRAMP
AWS IAM Identity Center	SOC 1, SOC 2, SOC 3, PCI DSS, HIPAA, IRAP, ISO 27001/17/18
AWS AppConfig	SOC 1, SOC 2, SOC 3, PCI DSS, HIPAA, ISO 27001/17/18, FedRAMP
AWS Organizations	SOC 1, SOC 2, SOC 3, PCI DSS, HIPAA, ISO 27001/17/18
Amazon RDS	SOC 1, SOC 2, SOC 3, PCI DSS, HIPAA/HITECH, ISO 27001/17/18, FedRAMP, GDPR
AWS Secrets Manager	SOC 1, SOC 2, SOC 3, PCI DSS, HIPAA, ISO 27001/17/18, ISO 9001
AWS Lambda	SOC 1, SOC 2, SOC 3, PCI DSS, HIPAA, FedRAMP, ISO 27001/17/18
AWS CodeBuild	SOC 1, SOC 2, SOC 3, PCI DSS, HIPAA, FedRAMP, ISO 27001/17/18
Amazon S3	SOC 1, SOC 2, SOC 3, PCI DSS, HIPAA/HITECH, ISO 27001/17/18, FedRAMP, GDPR
AWS Key Management Service (KMS)	SOC 1, SOC 2, SOC 3, PCI DSS, HIPAA, FedRAMP, ISO 27001/17/18, FIPS 140-3
Amazon Simple Queue Service (SQS)	SOC 1, SOC 2, SOC 3, PCI DSS, HIPAA, ISO 27001/17/18, FedRAMP

Service	Certifications
AWS Systems Manager	SOC 1, SOC 2, SOC 3, PCI DSS, HIPAA, FedRAMP, ISO 27001/17/18
Amazon CloudWatch	SOC 1, SOC 2, SOC 3, PCI DSS, HIPAA, FedRAMP, ISO 27001/17/18

For official audit reports and current scope, use **AWS Artifact** or consult the **AWS Services in Scope by Compliance Program** documentation.

Summary

Sandbox Studio is designed with **security-first principles** and built on **compliant AWS services** . Key assurances include:

- Complete customer control of data, identity, and network boundaries.
- End-to-end encryption, least-privilege IAM roles, and enforced SCP guardrails.
- Defence-in-depth VPC design with layered subnets and strict egress rules.
- Strong network protection via AWS WAF and CloudFront TLS enforcement.
- Automated account lifecycle management with auditable teardown.
- Monitoring and governance integrated with AWS-native services.
- Foundation aligned with **ISO 27001, SOC 2, PCI DSS, HIPAA, and FedRAMP-certified AWS services**.

This model provides **security officers and auditors confidence** that sandbox environments are **isolated, compliant, and tightly governed** — enabling safe innovation in AWS without introducing enterprise risk.

Revision #4
Created 2025-08-24 07:01:32 UTC by Andy
Updated 2025-08-27 09:44:26 UTC by Andy