OmniSite Cybersecurity & Compliance Overview (AWS-Hosted)

Audience: Enterprise security, compliance, and procurement teams
Purpose: Explain how OmniSite secures customer data and services on Amazon Web Services (AWS), how responsibilities are shared, and how our controls align to common frameworks.

---

1) Scope & Architecture Context

- **Primary Region:** US-EAST-2 (Ohio). Workloads and data are hosted in this region unless otherwise contracted.
- **Compute & Orchestration:**
- **Amazon EKS** runs our APIs, front-end applications, packet processing services, and notification delivery workers.
- **Amazon ECS** handles high-throughput packet ingestion; ingested messages are published to **Amazon SQS** for durable, decoupled processing by EKS workloads.
- **Data layer: Amazon RDS** (Multi-AZ) for relational databases and transaction processing; read replicas/restore options per tier.
- **Observability:** 24/7 monitoring via **Amazon CloudWatch** and **Zabbix**.
- **Operations:** 24/7/365 on-call coverage by OmniSite; **Mission Cloud** (AWS Premier partner) provides additional anomaly monitoring across data flows and web traffic.

  Note: Our previous on-prem/colocation materials (e.g., facility summaries from earlier providers) are superseded by this document.

---

2) Shared Responsibility Model (Who does what)

Security and compliance are a **shared responsibility** between OmniSite (the customer of AWS) and AWS (the cloud provider).

- **AWS is responsible for** security **of** the cloud: global infrastructure, facilities, hardware, and managed service baselines (e.g., host OS for managed databases).
- **OmniSite is responsible for** security **in** the cloud: identity and access, network controls, OS/app hardening for IaaS, data classification and encryption choices, logging/monitoring configuration, secure SDLC, backup/DR, and incident response.

This division allows us to focus on application-layer security while leveraging AWS's rigor for infrastructure security.

---

3) AWS Global Infrastructure & Physical Security (Inherited Controls)

OmniSite inherits AWS's physical and environmental safeguards, including:
- 24×7 staffed data centers with perimeter/in-building controls, video surveillance, intrusion detection, and strict access procedures.
- Redundant power (UPS/generators), fire detection and suppression, and climate controls to maintain availability.
- Media sanitization processes and structured device decommissioning.
- Business continuity measures at the infrastructure layer across multiple Availability Zones.

For customers, this means OmniSite builds atop a hardened, highly available foundation.

---

4) OmniSite Security Controls (Operating in the Cloud)

4.1 Identity, Access, and Account Security

- **Least privilege IAM:** Role-based access with granular permissions; separation of duties for operations and deployments.
- **Strong authentication:** MFA enforced for privileged access; short-lived credentials for automation where supported.
- **Key management:** AWS KMS customer keys for data encryption; controlled access, rotation, and monitoring.

4.2 Network Security

- **Segmentation and isolation:** Dedicated VPCs, subnets, and security groups; least-privilege network paths.
- **Perimeter controls:** Managed load balancers and WAF (where applicable); ingress/egress restrictions; private endpoints for internal services.
- **Secret handling:** No plaintext secrets in code repositories; secrets stored in AWS Secrets Manager/ Parameter Store with audit trails.

4.3 Data Protection

- **Encryption in transit:** TLS for service-to-service and client connections; modern cipher suites.
- **Encryption at rest:** Service-level encryption for storage, databases, and backups.
- **Data lifecycle:** Retention policies per product and contract; secure deletion procedures for ephemeral artifacts.

4.4 Logging, Monitoring, and Detection

- **Centralized activity logging:** AWS CloudTrail for API/control-plane events; CloudWatch Logs for application and system telemetry.
- **Metrics & dashboards:** CloudWatch metrics/alarms for infrastructure and services; **Zabbix** for supplemental host/service health and custom checks.

- **Continuous assessment:** AWS Config rules/conformance packs to detect drift from baselines.
- **Threat detection & anomaly monitoring:** AWS GuardDuty (where enabled) for threat findings; **Mission Cloud** provides 24/7 anomaly monitoring of data flows and web traffic with escalation to OmniSite on-call. Mission Cloud's managed services operate under a SOC 2 Type II program (Security & Availability) with independent third-party examination.
- **Alerting & response:** Alarms routed to the 24/7/365 on-call rotation with documented playbooks for triage and escalation.

4.5 Vulnerability & Patch Management Vulnerability & Patch Management

- **OS & image hygiene:** Golden AMIs/containers with routine patching and CIS-aligned hardening where appropriate.
- **Dependency management:** Automated scanning of container images and third-party libraries; remediation SLAs based on severity.
- **Change management:** Peer review, CI/CD checks, and progressive delivery to reduce blast radius.

4.6 Secure SDLC

- **Static/dynamic analysis:** Security checks integrated into build pipelines.
- **Secrets scanning:** Automated scanning in repositories and container images.
- **Code review:** Mandatory reviews for sensitive changes; protected branches and signed artifacts where applicable.

4.7 Backup, Restore, and Disaster Recovery

- **Backups & versioning:** Scheduled snapshots/backups for critical data stores; cross-AZ replication for durability.
- **RDS Multi-AZ:** Automatic failover capability for database availability; routine restore tests validate recoverability.
- **EKS multi-AZ design:** Node groups and workloads deployed across multiple Availability Zones to reduce single-AZ risk.
- **DR objectives:** Documented RTO/RPO targets by system tier; periodic recovery tests.
- **Runbooks:** Standard operating procedures for restore and failover.

4.8 Incident Response

- **Preparation:** 24×7 monitoring, contacts, and communication channels.
- **Triage & containment:** Well-defined roles, isolation options, credential revocation, and traffic filtering.
- **Eradication & recovery:** Patch, rebuild, or rotate as needed; verify integrity before restoration.
- **Post-incident:** Root-cause analysis, corrective actions, and customer notifications per contractual/legal requirements.

---

5) Compliance Alignment

OmniSite leverages AWS's third-party audits and certifications (e.g., SOC, ISO 27001 family, PCI DSS scope for managed services, FedRAMP where applicable) and layers OmniSite's own organizational and technical controls on top.

- **Inherited controls:** Physical security, infrastructure operations, and many managed-service baselines are covered by AWS attestations.
- **Mission Cloud assurance:** Mission Cloud maintains a **SOC 2 Type II** program covering **Security and Availability**, with an independent audit by BARR Advisory for the period **August 1, 2024 – July 31, 2025**. Mission Cloud also issues a current bridge letter stating there were **no material changes** to its information security control structure that would adversely affect the prior auditor's opinion for the period **August 1, 2024 – October 27, 2025**.
- **Customer-specific attestations:** Upon request and where under NDA, OmniSite can reference relevant Mission Cloud SOC materials and AWS compliance resources to support assessments.
- **OmniSite controls mapping:** We provide controls narratives and can complete customer security questionnaires (e.g., SIG/CAIQ) mapping OmniSite practices to frameworks (NIST CSF, SOC 2 CCs, ISO 27001 Annex A, CIS).

---

6) Customer Data Responsibilities

While OmniSite secures the platform and managed application services, customers remain responsible for:
- Safeguarding their credentials and MFA for tenant-level access.
- Managing end-user authorization and least privilege within their org.
- Classifying data and using provided controls (e.g., role scoping, API keys, rotation).
- Following recommended client/network safeguards within their environment.

---

7) Business Continuity & Service Availability

- **Multi-AZ architectures:** EKS node groups and critical services span multiple AZs; **RDS Multi-AZ** for database high availability.
- **Decoupled processing: SQS** buffers bursts and isolates producers from consumers; **ECS → SQS → EKS** flow provides elasticity and failure isolation.
- **Scaling & replacement:** Automated scaling and self-healing for containerized workloads; immutable deployments minimize configuration drift.
- **Operational readiness:** 24/7/365 on-call coverage; Mission Cloud co-monitoring and joint incident procedures.
- **Exercises:** Routine game-days and restoration drills to validate RTO/RPO targets.

---

8) Requests from Customer Security Teams

We routinely support security diligence by providing:
- Completed security questionnaires (SIG/CAIQ or customer-supplied).
- Architectural/data-flow diagrams under NDA.
- Details on encryption, key management, logging, retention, and incident practices.
- References to relevant AWS audit reports and compliance pages.

Appendix A — Mission Cloud SOC 2 (Summary for Reviewers)

Purpose: Provide a concise overview of Mission Cloud's SOC 2 materials that support OmniSite's co-monitoring model and control environment assertions.

A.1 Report Scope (Type II; Trust Services Criteria)

- **Report type & period:** SOC 2 Type II covering **Security** and **Availability** for the period **Aug 1, 2024 – Jul 31, 2025**.
- **Independent auditor:** BARR Advisory.
- **Control coverage:** Managed services and supporting processes forming Mission Cloud's control environment (governance, access, change, monitoring, incident management, and availability planning).

A.2 What Reviewers Will Find in the SOC 2 Report

- **Management assertion & system description:** Narrative of services in scope and responsibilities under the Shared Responsibility Model.
- **Control objectives & tests:** Detailed controls mapped to SOC 2 criteria with **auditor test procedures** and **results** (operating effectiveness across the audit period).
- **Complementary User Entity Controls (CUECs):** Responsibilities customers must implement for the controls to remain effective (e.g., enforcing least-privilege, timely incident notifications, change approvals).
- **Subservice organizations (if applicable):** Carve-outs and dependencies noted by the auditor.

A.3 How OmniSite Uses the SOC 2 Materials

- **Assurance layering:** We inherit assurance from Mission Cloud's audited practices for the co-managed portions of monitoring and operations, and from AWS for physical/infrastructure controls; OmniSite's own controls govern application/data layers.
- **Evidence referencing:** Under NDA, we can reference sections of the Mission Cloud SOC 2 to answer customer questionnaires related to monitoring, incident response, and availability.

Appendix B — Bridge Letter (How to Use)

Purpose: Explain how the bridge letter complements the SOC 2 report for periods after the report end date.

B.1 What the Bridge Letter States

- Confirms **no material changes** to Mission Cloud's control environment that would adversely affect the prior SOC 2 auditor's opinion, for the period following the report end date through the bridge letter date.

B.2 How Reviewers Should Apply It

- **Continuity of assurance:** Use the bridge letter to extend reliance **from Aug 1, 2024 – Jul 31, 2025** through **Oct 27, 2025** (or current letter date), pending issuance of the next SOC 2 report.
- **Scope check:** Verify that your due-diligence window falls within the SOC 2 period **plus** the bridge letter coverage.
- **Limitations:** The bridge letter is not a full audit; it supplements the SOC 2 report and should be read alongside it.