**Cloud Security & Data Privacy Policy (CSDP v1.0)**

**Classification:** Internal Use / Confidential  
**Policy Owner:** Chief Information Security Officer (CISO) – Keitavius Alexander  
**Department:** Cloud Governance, Security & Compliance  
**Effective Date:** 10/16/2025  
**Last Reviewed:** 10/16/2025  
**Next Review Date:** 10/16/2026  
**Approved By:** Cloud Governance and Risk Oversight Committee

**Table of Contents**

1. Executive Summary
2. Purpose
3. Scope
4. Policy Statement
5. Roles and Responsibilities
6. Policy Requirements
   * 6.1 Zero Trust Access Control
   * 6.2 Data Protection and Encryption
   * 6.3 Network and Infrastructure Security
   * 6.4 Monitoring, Logging, and Anomaly Detection
   * 6.5 Dual-Layer Incident Response
   * 6.6 Backup and Resiliency
   * 6.7 Vendor and Third-Party Oversight
7. Strategic Impact and Value
8. Enforcement and Compliance
9. References and Framework Alignment
10. Appendices

* 10.1 Key Definitions and Acronyms
* 10.2 Version Control and Approval Record
* 10.3 Regulatory and Framework Alignment Map
* 10.4 Sample Incident Response Workflow
* 10.5 Policy Intent and Summary

**1. Executive Summary**

The Cloud Security & Data Privacy Policy (CSDP) establishes the organization’s governance and control framework for securing all cloud-hosted data, systems, and services.  
This policy enforces Zero Trust principles, automated monitoring, sandboxing, and a dual-layer incident response structure to ensure operational resilience and regulatory compliance.  
By aligning with industry standards such as NIST CSF, ISO/IEC 27001, and CSA Cloud Controls, the policy strengthens trust among clients, regulators, and internal stakeholders.  
**Executive Note:** Effective cloud security is no longer optional; this policy ensures proactive defense, business continuity, and secure innovation without hindering productivity.

**2. Purpose**

The purpose of this policy is to:

* Protect organizational cloud environments, data, and services through proactive security controls and continuous monitoring.
* Implement Zero Trust architecture and least privilege access across all cloud systems.
* Safeguard sensitive and regulated data through encryption, segmentation, and privacy-by-design practices.
* Ensure timely, coordinated response and recovery during security incidents.
* Maintain compliance with regulatory and industry standards while supporting business agility.

**3. Scope**

This policy applies to:

* All employees, contractors, and third-party vendors interacting with organizational cloud infrastructure or SaaS platforms.
* All users of cloud-hosted applications, portals, or data services.
* Cloud deployments across IaaS, PaaS, and SaaS environments.
* Third-party service providers with access to cloud assets or sensitive data.

It governs all activities related to cloud security, data privacy, access control, monitoring, and incident response.

**4. Policy Statement**

The organization is committed to securing cloud environments through layered defense, data protection, and Zero Trust principles.  
All personnel must comply with this policy and its related standards. Non-compliance may result in disciplinary action, termination of access, or contractual penalties.

**5. Roles and Responsibilities**

* **Executive Leadership:** Approves this policy, allocates resources, and ensures organization-wide compliance.
* **Cloud Security & Compliance Team:** Implements Zero Trust controls, monitors activity, manages incident response, and audits logs.
* **IT / DevOps Operations:** Maintains firewall rules, VPC segmentation, encryption, and endpoint security.
* **Employees and Users:** Follow access controls, report anomalies, and comply with incident response guidance.
* **Vendors and Third Parties:** Adhere to cloud security requirements, provide audit evidence, and coordinate during incidents.

**6. Policy Requirements**

**6.1 Zero Trust Access Control**

* Principle: Never trust, always verify.
* All access requests must be dynamically validated through MFA, device checks, and behavioral analytics.
* Implement Role-Based Access Control (RBAC) and enforce least privilege.
* Continuously monitor sessions, users, and endpoints for anomalies.

**6.2 Data Protection and Encryption**

* Encrypt all data at rest using AES-256 and in transit using TLS 1.2 or higher.
* Classify and protect sensitive data (PII, PHI, financial, intellectual property) according to risk level.
* Manage encryption keys centrally with full auditability.
* Generate automated alerts for unauthorized data access or modification.

**6.3 Network and Infrastructure Security**

* Enforce firewalls, VPC segmentation, and private subnets to minimize exposure.
* Monitor inbound and outbound traffic with IDS/IPS systems.
* Require VPN and conditional access for administrative sessions.
* Log and review network activity continuously for analysis and investigation.

**6.4 Monitoring, Logging, and Anomaly Detection**

* Capture all cloud resource interactions through centralized logging.
* Enable automated alerts for unusual activity or violations.
* Conduct periodic behavioral analytics to detect emerging threats.
* Isolate anomalous activities in sandboxed environments for analysis.

**6.5 Dual-Layer Incident Response**

**Employee Response:**

1. Detection, classification, containment, eradication, recovery, and post-incident review.
2. Immediate escalation to the Cloud Security & Compliance Team for critical events.

**End-User Response:**

1. Instant alerts and guided response for detected anomalies.
2. Temporary account isolation, sandboxing, and automated remediation.
3. Transparent communication of resolution and lessons learned.

**6.6 Backup and Resiliency**

* Perform regular backups of critical systems and datasets.
* Define and test Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO).
* Prevent corrupted or anomalous data from entering production through sandbox integration.

**6.7 Vendor and Third-Party Oversight**

* Require all vendors to comply with this policy and provide evidence of SOC 2 or ISO 27001 certification.
* Conduct regular vendor risk assessments and audits.
* Enforce contractual SLA and DSA requirements to maintain accountability.

**7. Strategic Impact and Value**

* **Risk Reduction:** Minimizes exposure to data breaches, insider threats, and service outages.
* **Operational Continuity:** Sandboxing, redundancy, and incident response ensure system resilience.
* **User Trust:** Transparent communication and responsive security strengthen stakeholder confidence.
* **Compliance:** Aligns with NIST CSF, ISO/IEC 27001, CSA Cloud Controls, and Zero Trust standards.
* **Innovation Enablement:** Enables teams to innovate securely without compromising compliance.

**8. Enforcement and Compliance**

* Violations by employees or contractors may result in disciplinary action, access termination, or legal review.
* Vendors failing to meet requirements may face immediate contract suspension or termination.
* The organization reserves the right to audit and update this policy as technologies and threats evolve.

**9. References and Framework Alignment**

* NIST Cybersecurity Framework (CSF)
* ISO/IEC 27001 – Information Security Management Systems
* Cloud Security Alliance (CSA) Cloud Controls Matrix
* Zero Trust Architecture Guidelines
* SOC 2 – Trust Services Criteria

**10. Appendices**

**10.1 Key Definitions and Acronyms**

Includes standardized terms such as RBAC, MFA, IDS/IPS, DSA, VPN, and Zero Trust.

**10.2 Version Control and Approval Record**

Tracks revisions, approval dates, and responsible parties for audit traceability.

**10.3 Regulatory and Framework Alignment Map**

Maps each control requirement to NIST CSF, ISO 27001, and CSA CCM domains.

**10.4 Sample Incident Response Workflow**

Provides a visual or textual escalation path with defined response timelines.

**10.5 Policy Intent and Summary**

Reiterates the organization’s commitment to secure, compliant, and resilient cloud operations.