Kemicard SOC 2 Compliance Policy

Overview

Kemicard is a Salesforce-native application developed and managed by Kemisoft. As an Independent Software Vendor (ISV), we operate entirely within the Salesforce Platform—leveraging its infrastructure, data centers, and security controls. While Kemisoft does not currently hold an independent SOC 2 or ISO 27001 certification, Kemicard inherits the comprehensive security and compliance posture of the Salesforce ecosystem.

Salesforce maintains full **SOC 1 Type II** and **SOC 2 Type II** certifications, along with **ISO 27001**, **PCI DSS**, and additional third-party attestations. These certifications verify that Salesforce's internal controls, policies, and systems meet rigorous industry standards for security, availability, processing integrity, confidentiality, and privacy.

Alignment with Salesforce SOC 2 Controls

Kemicard's architecture, data storage, and transaction processing are fully hosted and executed within the Salesforce environment. This ensures that:

- **Data security and privacy** controls adhere to the same standards audited under Salesforce's SOC 2 Type II framework.
- **Availability and reliability** are maintained through Salesforce's globally redundant infrastructure and uptime SLAs.
- **Access management** follows Salesforce's permission-based model, including authentication, audit logging, and encryption in transit and at rest.

- **Processing integrity** is supported by Salesforce's continuous monitoring, automated testing, and compliance-driven development processes.

- **Confidentiality and privacy** are safeguarded by Salesforce's data governance policies, encryption frameworks, and regional compliance adherence (including GDPR and CCPA).

Kemicard's Internal Commitments

Beyond Salesforce's inherited controls, Kemisoft implements internal practices that strengthen our alignment with SOC 2 principles:

- **Change Management** – All updates and deployments to Kemicard follow Salesforce's AppExchange security review process.

- **Data Handling** – Kemicard does not move or store customer data outside the Salesforce Platform.

- **Access Control** – Administrative access to production environments is restricted to authorized personnel only, governed by least-privilege principles.

- **Monitoring & Incident Response** – We actively monitor application performance and rely on Salesforce's native alerting and event logging for real-time incident visibility.

- **Continuous Improvement** – Kemisoft reviews Salesforce's compliance updates and integrates relevant best practices into our operational and development procedures.

Customer Assurance

By deploying Kemicard, customers benefit from the same enterprise-grade security, privacy, and availability standards that govern Salesforce's SOC 2 Type II environment. Our reliance on Salesforce's certified infrastructure ensures that customer data is protected with the highest level of control and transparency available in the cloud ecosystem.

For customers requiring further assurance, Salesforce's most recent **SOC 2 Type II report** and supporting documentation can be requested directly from Salesforce via their **Trust and Compliance Documentation Portal**.

Conclusion

Kemicard’s security posture is rooted in the proven, audited, and continuously monitored infrastructure of Salesforce. While Kemisoft is not independently SOC 2 certified, our full operational dependence on Salesforce’s compliant environment ensures that our customers benefit from a platform that meets the industry’s highest standards for data security and integrity.