

Concentric AI Service Definition

Confidentiality Notice

This document and all included materials are confidential and intended solely for the recipient(s) participating in this G Cloud Submission. Distribution or disclosure of this information to any unauthorized individual or entity is strictly prohibited without prior written consent from Concentric AI.

Concentric.AI provides a software-as-a-service (“SaaS”) data security, governance, and risk management platform (the “**Service**”) that enables organizations to discover, classify, monitor, and protect sensitive, confidential, and regulated data across cloud, SaaS, and on-premises environments.

1. Scope and Purpose of the Service

The Service is designed to give customers visibility into the location, nature, access, and usage of their data and to support the protection of such data against unauthorized access, disclosure, misuse, loss, or policy violations. The Service supports data security posture management (DSPM), data governance, compliance, and data loss prevention use cases.

2. Data Discovery and Classification

The Service analyzes customer data stored within connected systems and repositories for the purpose of identifying and classifying data based on its content, context, and sensitivity. This includes both structured and unstructured data. Using artificial intelligence and machine-learning techniques, including semantic analysis, the Service identifies categories of data such as:

- Personal data and personal data subject to applicable data protection laws
- Confidential and proprietary business information
- Intellectual property
- Financial, legal, healthcare, or other regulated data

Classification is performed without reliance solely on static rules or keyword matching and is intended to improve accuracy, reduce false positives, and scale across large and diverse data environments.

3. Risk Identification and Monitoring

The Service continuously evaluates data access, permissions, sharing settings, and usage patterns to identify potential data security and governance risks. These risks may include, but are not limited to:

- Excessive or inappropriate access rights
- Over-sharing or public exposure of sensitive data
- Inconsistent or misaligned permissions
- Unauthorized access or anomalous behavior
- Policy or compliance violations

The Service generates alerts, insights, and reports to support customer review and decision-making.

4. Governance, Remediation, and Controls

The Service provides tools to support governance and remediation activities, including:

- Visibility into who has access to sensitive data and why

- Recommendations to reduce exposure or improve security posture
- Customer-initiated or automated actions to remediate identified risks (subject to configuration and permissions)

The Service does not independently modify customer systems or data unless explicitly authorized and configured by the customer.

5. GenAI and AI Usage Governance

Where enabled, the Service supports governance of data interactions with artificial intelligence and generative AI tools by detecting and assessing the sharing or movement of sensitive data to such services. This capability is intended to help customers manage risks associated with unauthorized or unintended disclosure of sensitive data in AI-enabled workflows.

6. Data Processing and Use Limitations

Concentric.AI processes customer data solely to provide, maintain, and improve the Service in accordance with the applicable agreement and documented customer instructions. Customer data is not used to train general-purpose artificial intelligence models or for purposes unrelated to the delivery of the Service.

7. Security Measures

The Service incorporates administrative, technical, and organizational safeguards designed to protect customer data against unauthorized access, disclosure, alteration, or destruction. These measures include controls relating to authentication, access management, logging, monitoring, and encryption of data in transit and at rest, as further described in Concentric.AI's security and compliance documentation.

8. Customer Responsibilities

The customer retains control over its data, including decisions regarding system connections, access permissions, configurations, and remediation actions. The customer is responsible for ensuring that its use of the Service complies with applicable laws, regulations, and contractual obligations.