Information Security Policy Summary

Overview

Daedalus AI Holdings LLC (“Daedalus”) maintains a formal Information Security Policy and structured security governance program designed to protect the confidentiality, integrity, and availability of information processed through our enterprise software platform, artificial intelligence–enabled systems, managed services, APIs, and on-premise deployments.

This summary provides an overview of the principles, governance structure, and control domains reflected in our internal Information Security Policy. The full policy is maintained as a controlled document and is available to customers under appropriate confidentiality protections.

Governance and Executive Oversight

Information security at Daedalus is governed at the executive level and is treated as a core enterprise risk function. Executive leadership provides oversight of the security program, ensures appropriate allocation of resources, and supports enforcement of security controls across the organization.

Daedalus designates a Security Officer responsible for administration of the information security program, including risk management, policy maintenance, incident response coordination, and ongoing improvement of security controls.

Risk Management

Daedalus maintains a formal risk management process designed to identify, assess, prioritize, and mitigate risks to information assets and infrastructure. Risk assessments are conducted periodically and upon material changes to systems or operations.

Security risks are documented, evaluated for potential impact, and remediated or formally accepted based on defined governance procedures.

Protection of Customer Data

Daedalus applies layered administrative, technical, and organizational safeguards to protect Customer Data. Our internal Information Security Policy addresses data classification, data minimization, retention controls, and secure deletion practices.

Customer Data processed within Daedalus-controlled environments is encrypted in transit using industry-standard protocols and encrypted at rest using strong encryption standards.

Upon termination of a customer engagement, data is deleted in accordance with contractual commitments and applicable industry standards designed to render information irretrievable in the ordinary course of business.

Access Control and Identity Management

Access to systems and Customer Data is governed by least privilege principles and role-based access controls. Access is granted only to authorized personnel with a legitimate business need and is subject to periodic review.

Multi-factor authentication is required for privileged access and production system access. Documented procedures govern onboarding, role changes, and termination to ensure timely modification or revocation of access rights.

Secure Development Practices

Daedalus maintains a secure development lifecycle framework that integrates security considerations into design, development, testing, and deployment processes. Code changes are subject to review and change management controls, and software dependencies are monitored for known vulnerabilities.

Production, staging, and development environments are logically segregated to reduce risk of unauthorized changes or data exposure.

Monitoring and Incident Response

Daedalus maintains logging and monitoring capabilities designed to detect unauthorized access and anomalous activity within systems under our control. Security events are evaluated and escalated in accordance with documented incident response procedures.

In the event of a confirmed security incident affecting Customer Data, Daedalus provides notification consistent with contractual commitments and applicable law and undertakes containment and remediation actions.

Business Continuity and Resilience

Daedalus maintains a business continuity and disaster recovery framework designed to sustain critical operations and restore services following disruptive events. Disaster recovery procedures are periodically reviewed and tested.

Unless expressly stated in a customer agreement, specific recovery time or recovery point objectives are not guaranteed.

Third-Party Risk Management

Daedalus evaluates third-party service providers that may access or process Customer Data and requires such providers to maintain security safeguards consistent with contractual and regulatory expectations.

Daedalus remains responsible for ensuring that subprocessors meet applicable security requirements when processing Customer Data on our behalf.

AI-Specific Safeguards

Daedalus' artificial intelligence–enabled systems are designed with defined system boundaries and logical data separation controls. Customer Data is not used to train generalized artificial intelligence models.

AI-generated outputs require human review and validation prior to operational deployment. Customers retain responsibility for evaluating and approving outputs prior to use in production environments.

Regulatory and Industry Alignment

Daedalus' information security program is designed to support contractual and regulatory expectations applicable to enterprise, financial institution, healthcare, and government customers.

While Daedalus may align internal controls with recognized industry standards and frameworks, such alignment does not constitute formal certification unless expressly stated.

Continuous Improvement

Information security at Daedalus is treated as an ongoing governance discipline. Policies and controls are reviewed periodically to address evolving threats, regulatory developments, and operational changes.

Contact

For additional information regarding Daedalus' security practices, customers and prospective customers may contact:

legal@trydaedalus.ai

Daedalus AI Holdings LLC
1919 West Greenleaf
Chicago, Illinois 60626

Effective Date: January 1, 2026
Last Updated: March 2, 2026