Oodaloo Security, Privacy, and Data Protection Policy

Effective Date: August 21, 2025

Oodaloo is committed to protecting customer data and maintaining strong information security and privacy practices. This document outlines our policies and procedures in compliance with Plaid's requirements.

---

1. Governance & Responsibility

- The **Founder/CEO** serves as the Information Security Officer.
- Security issues may be reported to **security@oodaloo.io**.
- Responsibilities include oversight of access control, risk management, and incident response.

---

2. Information Security Policy

- Oodaloo maintains an operational security program that is continuously improved.
- Risks are identified through cloud provider updates, dependency scanning, and periodic access reviews.
- Security practices are reviewed quarterly and updated as needed.

---

3. Identity & Access Management

- **Role-Based Access Control (RBAC):** Access to production assets is granted only as required by job function.
- **Periodic Access Reviews:** Access rights are reviewed quarterly.
- **De-Provisioning:** Access is revoked immediately upon employee/contractor termination.
- **MFA:** Multi-factor authentication is required for all administrative and infrastructure accounts.

---

4. Encryption Practices

- **In Transit:** All data is encrypted using TLS 1.2 or higher.
- **At Rest:** All customer data, including data retrieved from Plaid, is encrypted using AES-256 with AWS Key Management Service.

---

5. Multi-Factor Authentication (MFA)

- **For Consumers:** Plaid Link provides MFA during bank authentication. Oodaloo does not store banking credentials.
- **For Systems:** Oodaloo requires MFA (e.g., SMS, authenticator apps) for access to cloud services and production infrastructure.

---

6. Vulnerability & Development Practices

- Oodaloo performs vulnerability scans against production assets and employee devices.
- Identified vulnerabilities are patched promptly within defined service levels.
- End-of-life (EOL) software is monitored and replaced.

- Source code is reviewed for security vulnerabilities as part of development.

---

7. Data Privacy & Consent

- **Consent:** Users provide explicit consent before Oodaloo collects or processes data.
- **Use Limitation:** Data is used exclusively to provide Oodaloo services (e.g., reconciliation, profitability analysis).
- **No Sharing:** Oodaloo does not sell or share customer data with third parties except as required by law.
- **Transparency:** This Privacy Policy is displayed to users in the application.

---

8. Data Retention & Deletion

- Data is retained only as long as required to deliver services.
- Users may request deletion at any time by contacting **support@oodaloo.com**.
- Deletion requests are processed promptly and confirmed to the user.
- Retention policies are periodically reviewed for compliance with applicable laws.

---

9. Incident Response

- In the event of a security incident involving customer data, Oodaloo will:
    1. Contain and investigate the incident.
    2. Notify affected users without undue delay.
    3. Document the root cause and remediation steps.

10. Privacy Contact

For privacy or security inquiries, contact:
Email: security@oodaloo.io
Address: Oodaloo, Greenville, SC