DoTRyT LLC — Security & Compliance Policy

Effective Date: February 28, 2025
Last Updated: February 28, 2025

At **DoTRyT LLC** ("**DoTRyT**," "**we**," "**us**"), safeguarding data and ensuring compliance are core to how we operate. This Security & Compliance Policy outlines our commitments to protecting information entrusted to us and supporting our Users' compliance needs.

---

1. Information Security Principles

- **Confidentiality**: We restrict access to data to authorized personnel only, using **role-based access controls (RBAC)** and multi-factor authentication (MFA).
- **Integrity**: We employ monitoring, logging, and auditing tools to ensure the integrity of systems and data.
- **Availability**: While DoTRyT does not guarantee uptime (see our Service Level Disclaimer), we strive for **99% availability** and maintain backup, redundancy, and disaster recovery measures.

---

2. Data Protection & Encryption

- All data in transit is encrypted using **TLS 1.2+**.
- All data at rest is encrypted with industry-standard AES-256 encryption.
- Access to production systems is restricted, logged, and monitored.

---

3. Compliance & Certifications

- DoTRyT is committed to meeting applicable regulatory, contractual, and industry requirements, including but not limited to:
    - **SOC 2 Type II** (in progress)

- **FedRAMP Moderate Ready** certification efforts (planned 2026)
- **CMMC Level 2** (for DoD-related contracts, in progress)
- Compliance with **U.S. privacy laws** (including Florida Digital Bill of Rights, CCPA) and **GDPR principles** for international Users.

---

4. User Responsibilities

- Users are solely responsible for ensuring their own compliance with government procurement laws, regulations, and contractual obligations.
- Users must not upload sensitive, classified, or prohibited content without proper authorization.
- Users are responsible for reviewing and validating all AI-generated outputs before use in bids or submissions.

---

5. Incident Response & Notifications

- DoTRyT maintains an **Incident Response Plan** to address security events and system outages.
- In the event of a confirmed data breach involving personal information, we will provide timely notifications in accordance with applicable law.

---

6. Continuous Improvement

- We regularly update our systems, infrastructure, and security practices.
- We conduct internal reviews, vulnerability scanning, and third-party assessments as appropriate.
- We reserve the right to **modify, update, or replace** security practices or compliance programs as needed to reflect evolving risks, standards, or regulations.

---

7. Contact Information

If you have questions regarding security, compliance, or wish to report a concern, please contact us:

DoTRyT LLC
Email: sales@dotryt.com