TITANIA

Information Security Statement

Version 1.0

[DOCUMENT CLASSIFICATION: CONFIDENTIAL]

Information Security Statement

At Titania, protecting the confidentiality, integrity, and availability of information is a core priority. Titania is committed to maintaining robust security practices to safeguard our systems, services, and the information entrusted to it by its customers, partners, and stakeholders.

Titania's security program is designed to identify and manage risks, implement appropriate safeguards, and continuously improve its security posture in response to evolving threats and business needs.

This Information Security Statement is provided for general information and assurance purposes only. It does not form part of the EULA or any agreement between Titania and its Licensees, Suppliers or Partners, unless expressly incorporated by reference.

1. Security Governance

Titania maintains a structured information security program supported by internal policies, procedures, and risk management processes. These are designed to ensure that security responsibilities are clearly defined and consistently applied across the organization.

Titania's security governance framework includes:

- defined information security roles and responsibilities;
- regular risk assessments and review activities;
- security awareness and training for employees; and
- information security policies aligned with recognized industry standards.

2. Data Protection

Titania implements appropriate technical and organizational safeguards to protect sensitive information and personal data from unauthorized access, alteration, disclosure, or destruction.

Security measures include:

- encryption of data in transit using industry-standard protocols;
- encryption of sensitive data at rest, where appropriate;
- role-based access controls and authentication mechanisms; and
- application of the principle of least-privilege access.

Security controls are selected and applied based on a risk-based assessment, taking into account the nature of the information, the processing context, and the potential impact of a security incident.

3. Infrastructure & Application Security

Titania's infrastructure and applications are designed with security in mind and are regularly reviewed to address vulnerabilities and emerging threats.

Controls include:

- secure system configuration and patch management;
- monitoring and logging of system activity;
- vulnerability assessments and remediation processes; and
- secure development practices, including code review.

Titania also maintains business continuity and recovery arrangements designed to support the ongoing availability of its services.

For the avoidance of doubt, the security of offline, air-gapped and Licensee-controlled environments remain the responsibility of the Licensee, including configuration, access control, and operational security.

4. Incident Detection & Response

Titania maintains procedures for detecting, responding to, and managing security incidents. Titania's incident response processes are designed to support timely containment, minimize impact, and enable secure recovery.

In the event of a security incident affecting Licensee data, Titania will respond in accordance with its internal policies and applicable legal and regulatory requirements.

5. Third-Party Risk Management

Where third-party vendors or service providers are used and may have access to Titania or Licensee systems or information, Titania assesses their security posture to ensure they meet appropriate security standards and contractual safeguards are in place.

6. Compliance & Standards

Titania's information security practices are informed by recognized industry frameworks and regulatory requirements, which include:

- ISO 27001
- GDPR and applicable data protection laws

Evidence of Titania's certifications may be made available to its Licensees upon reasonable request as part of Titania's due-diligence processes.

7. Continuous Improvement

Information security is an ongoing process. Titania regularly reviews and updates its policies, procedures, and technical controls to address new threats, vulnerabilities, and regulatory developments and to support the continued effectiveness of its security program.

8. Responsible Disclosure & Bug Bounty

Titania encourages the responsible reporting of potential security vulnerabilities. Suspected vulnerabilities must be submitted to security@titania.com with sufficient detail to allow for verification and investigation.

Titania does not operate a public bug bounty or vulnerability reward program. Submission of a report does not create any entitlement to compensation, nor does it grant any right or authorization to access, probe, or interfere with Titania systems beyond what is strictly necessary to identify the issue. Any activity that violates applicable law or compromises the confidentiality, integrity, or availability of Titania systems may be referred to competent authorities.

9. Disclaimer

While Titania implements strong security practices, no system can be guaranteed to be completely secure. Titania continuously works to improve its security posture and protect the information entrusted to it.