Information Security Statement for Laius Group

Effective Date: June 22, 2025
Last Reviewed: June 22, 2025

Laius Group (“we,” “our,” or “the Company”) is committed to maintaining the confidentiality, integrity, and availability of the information we manage on behalf of our users. While Laius Group is not officially certified under ISO 27001 or any other formal information security standard, we rigorously follow best practices and principles aligned with internationally recognized frameworks, including ISO 27001 and SOC 2, to safeguard our systems and data.

Risk Assessment for Laius Vaultspace

The Laius Vaultspace database, which securely stores all user login credentials, is considered a critical asset. We have identified potential threats including unauthorized access, data breaches, VPS compromises, and insider threats. Vulnerabilities associated with this asset include a limited number of administrators granted SSH key access, which, while tightly controlled, could present risks if key material is lost or compromised. Additionally, our security posture depends on the Vultr datacenter’s controls and proper configuration of IP whitelisting mechanisms.

To mitigate these risks, we have implemented the following controls:

- Access to Laius Vaultspace is restricted exclusively to official Laius Group Virtual Private Servers (VPS) via strict IP whitelisting.
- SSH key-based access is limited to a select group of experienced, high-level Laius Group administrators.
- Continuous real-time monitoring of SSH login attempts is enforced, with immediate alerts triggered by failed or suspicious activity.
- Laius Vaultspace is hosted within the Vultr Amsterdam datacenter, which maintains compliance with SOC 2 and ISO 27001 standards. Documentation of Vultr’s compliance certifications is available upon request.
- We conduct regular reviews and audits of access permissions, IP whitelist configurations, and SSH key usage to maintain security hygiene.
- Robust backup and recovery procedures are in place to ensure data availability and integrity in case of an incident.

Incident Response for Laius Vaultspace

In the event of a security incident involving Laius Vaultspace, we adhere to the following response procedures:

- Detect: Employ real-time monitoring systems to identify and alert on abnormal SSH login attempts immediately.

- Report: Notify the designated trusted administrators without delay upon detection of suspicious access attempts or anomalies.

- Assess: Promptly analyze system logs and security events to determine whether an incident is occurring or if activity is benign.

- Contain: Implement containment measures such as revoking or rotating compromised SSH keys, tightening IP whitelist settings, or isolating the affected Vaultspace instance as necessary.

- Eradicate: Remove any identified attack vectors, rotate all implicated SSH keys, and reset relevant credentials to eliminate persistent threats.

- Recover: Restore affected data from verified backups to return systems to a secure and operational state.

- Review: Conduct a comprehensive post-incident review to identify root causes, evaluate response effectiveness, and update security policies and controls accordingly.