Backup & Recovery Policy for Laius Group

Effective Date: June 26, 2025
Last Reviewed: June 26, 2025

Laius Group (“we,” “our,” or “the Company”) is committed to ensuring the resilience, integrity, and availability of all critical systems and data under our management. Although Laius Group is not officially certified under ISO 27001 or SOC 2, we adhere to industry-standard practices aligned with both frameworks to minimize the risk of data loss and service disruption.

Backup Strategy
We follow the 3-2-1 backup methodology to protect critical information assets. This includes maintaining at least three copies of data, storing them on two different types of media, with at least one copy stored offsite or isolated from the primary infrastructure.

The following backup schedules are maintained for key services:

- **Laius Connect (Authentication & Dashboard Service):** Daily full backups
- **Laius Echo (Mail Services):** Daily full backups
- **Laius Webfront (Public Website):** Weekly full backups

In addition to scheduled backups, immediate backups are executed following any internal system changes, including but not limited to configuration updates, infrastructure changes, and code or content deployments.

Storage & Redundancy
All backups are encrypted and stored securely in geographically diverse locations to ensure redundancy and protection against localized failures. Backups are retained according to the criticality of each system and follow defined retention periods appropriate to operational and legal needs.

Access Control & Monitoring
Access to backup systems is strictly limited to designated Laius Group administrators with relevant roles and responsibilities. Audit logs are maintained, and backup integrity is regularly verified through restoration testing.

Disaster Recovery & Restoration
In the event of a data loss or corruption scenario, recovery procedures are initiated immediately. Restoration processes are documented and periodically tested to confirm the recoverability of systems within acceptable Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO).

We maintain one failover server for Laius Webfront to ensure continuity in the event of a production outage.

This policy will be reviewed regularly and updated as necessary to reflect changes in infrastructure, regulations, or operational requirements.