Validator Security Policies

Validator Information

Validator Name:	Asuga
Cluster:	mainnet-beta
Website:	`https://asuganodes.com`

1 Infrastructure Overview

Hosting Provider:	Edgevana
Server Location:	Frankfurt, Germany
Redundancy:	Backup infrastructure in place to ensure validator uptime and fast recovery
Monitoring:	Real-time monitoring and alerting powered by DataDog

2 Security Practices

2.1 Key Management

- Validator identity key is stored offline in secure, air-gapped storage.
- Vote and authorized withdrawal keys are stored securely with restricted access.
- All keys are backed up in encrypted form, with access limited to trusted personnel.

2.2 Firewall and Network Security

- Firewalls restrict access to only necessary Solana ports and secure SSH.
- SSH access is protected with public key authentication and IP whitelisting.
- Logs and access attempts are regularly reviewed for anomalies or intrusion attempts.

2.3 Software Security

- Validator runs the latest stable version of Solana software.
- Updates are tested on a non-critical node before deployment to mainnet.
- System and dependency packages are regularly patched for known vulnerabilities.

3 Incident Response

- Incidents such as downtime or suspected compromise are investigated promptly.
- If key compromise occurs, validator identity is revoked and replaced.
- Significant incidents will be communicated via our official Twitter account.

4 Contact

Security Contact:	`security@asuganodes.com`
Twitter:	`https://x.com/asuganodes`

5 Responsible Disclosure

We welcome responsible disclosure of any vulnerabilities or misconfigurations. Please contact us at the email above. Although we do not currently offer a formal bug bounty, we appreciate the contributions of the security community.