Security & Privacy FAQ

→ What security certifications and audits do you have?

Nodes & Links maintains ISO 27001 and UK Cyber Essentials credentials, which provide independent assurance that security controls meet global best practice standards. We also undertake penetration testing across the entire platform, performed by independent, certified experts. Relevant certificates are shared during formal infosec reviews.

→ What cloud architecture do you use?

The platform runs on AWS and uses logical tenant isolation enforced at the API and data layers to protect each customer's environment. We are able to host data by default to the USA, EU, UK and AUS. Additional regions are available upon request.

→ Do you use firewalls?

Yes—host-level firewalls are enabled on corporate endpoints, and network security controls align with ISO 27001 guidance for network protection.

→ Is customer data ever shared with others?

Customer data is never shared across customers, and confidentiality is governed by NDAs and strict authorization. Data is logically segmented at the datastore level with tenant identifiers enforced at the API layer so each customer can only access their own data.

→ How is customer and system data encrypted at rest and in transit?

All databases, data stores, and file systems are encrypted using AES-256, and all external data transmissions are end-to-end encrypted with TLS using strong protocols and ciphers. Keys are managed and rotated via AWS.

→ What is your backup and restore posture?

Backups of customer and system data are taken daily, encrypted like production data, replicated to a separate AWS region, and continuously monitored.

→ What access controls do you enforce?

Access follows role-based access control and the least-privilege principle with verified identity, unique accounts, annual access reviews, and mandatory MFA for privileged accounts.

→ How is software developed securely?

Security is embedded across all SDLC phases with threat modeling, code reviews, OWASP-aligned secure coding, segregation of environments, and independent testing in non-production environments.