Accelerus XUNO Information Security Measures

Accelerus is committed to safeguarding your data and we follow industry best practices to maintain strong, proactive security measures to protect the confidentiality, integrity, and availability of the information entrusted to us. For more details on our approach to information security, please see the information below.

1. Back ups

Accelerus has established backup policies. Backups are performed regularly and include a full copy of both data and system configurations. The backup status is reviewed monthly, and restoration tests are conducted on a random basis once per month to ensure reliability.

A defined backup retention policy is in place, structured as follows:

- Point-in-time backups retained for 35 days
- Weekly backups retained for 6 months
- Monthly backups retained for 1 year
- Annual backups retained for 10 years

Backups adhere to the retention policy and are stored in Azure Blob Cold Storage.

2. Encryption

Data encryption measures are in place to protect information both in transit and at rest. Data is encrypted using TLS 1.2, ensuring secure transmission between systems. All restful endpoints are secured with HTTPS-only connections, safeguarding stored data against unauthorized access.

3. Access Controls

The hosted Accelerus solution is securely hosted in an Azure cloud environment, which is fully segregated from the internal network. External access is restricted, with Azure administrators required to use Two-Factor Authentication (2FA) to log in.

Tiered access controls are in place, ensuring that users have appropriate levels of access. These controls align with Essential 8 Level 2 security standards to which Accelerus is certified. All users must authenticate to access the system, and strict measures are in place to control third-party access.

4. Security controls

Accelerus has established a data and incident breach management policy to ensure security incidents are handled effectively. Regular security and anti-virus scanning is conducted using Microsoft Defender, providing continuous monitoring and protection.

To maintain system security, annual penetration testing (pentesting) is performed, alongside frequent bug fixes and security patches. Updates and patches for known or exploitable vulnerabilities are actively managed, with security alerts received from pentest providers.

All known security risks and issues are documented and tracked using Azure DevOps, ensuring they are prioritized, fixed, tested, and delivered in a structured manner.