Axco Insurance Information Services Limited

Sub-processors

- **Pulsant**
  All systems are hosted by Pulsant, https://www.pulsant.com/, in their data centre in Reading and disaster recovery system in Milton Keynes.

  Pulsant is accredited with ISO/IEC 27001, CSASTAR, PCI-DSS Level 1 (physical security and remote hands) and is certified and audited every 6 months. As part of the ISO27001 accreditation, Pulsant employs a full time Information Security Manager who works as part of a larger compliance team.

  Pulsant has a centrally published Information Security policy and this policy, and the policy set that supports it are updated regularly to support improvements in policy and process. Client facing applications are all secure web sites using secure HTTP protocol using an SHA-256 certificate issued by a certified authority. All access to the Production environment is protected by a firewall. All data is held on a separate VLAN to the internet facing web servers. Pulsant utilises an internally hosted cloud-based backup system for both internal backups and customer backup solutions. Backups are transmitted across their core network to dedicated secure storage on suitable sites within their own infrastructure. Data is encrypted in transit.

  We employ a warm standby Disaster Recovery environment hosted in Pulsant's Milton Keynes data centre and take a daily backup from our database and when new code is deployed, we take a backup from the previous version in case anything goes wrong to enable us to revert should we need to.

- **Nasstar**
  IT Services are provided by Nasstar, http://www.nasstar.com, in their Tier 3 data centre in Telford, their secondary Tier 3 data centre is in London.

  Nasstar obtained the ISO 27001 certification in July 2010 and now operate an Information Management System to comply with ISO 27001:2013. To ensure compliance, Nasstar has documented every aspect of the business and has a dedicated portal for the storage and management of ISO 27001 policies and procedures. As part of the ISO27001 accreditation, Nasstar's dedicated Information Security Manager is responsible for ensuring staff compliance. Nasstar also publish a list of their compliance policies on their website.

  Nasstar runs monitoring software on our network and data leak prevention software on our email system which is reviewed internally by the IT Deliver Services team. The Nasstar ISMS is audited by an external Certification Body called SGS. Nasstar's data centres are built with N+1 architecture throughout providing full continuity of service and security.

- **Azure**
  Critical systems, including SQL servers, APIs, and front-end code, are hosted on Microsoft Azure. Azure also supports our development environment, which includes virtual machines, development servers and Azure DevOps for CI/CD.

Azure is accredited with key certifications like ISO/IEC 27001, PCI DSS, and others, reflecting its commitment to data protection and privacy. The platform ensures the safety of client-facing applications with advanced encryption and strict access controls.

In addition to hosting our production environment, Azure's versatile infrastructure facilitates our development processes, offering a scalable and secure platform for our developers to build and test applications efficiently.

Azure's comprehensive backup solutions and disaster recovery capabilities further fortify our data resilience, ensuring business continuity and data integrity across our operations.

- **Nagarro**
  Software Development Services are provided by Nagarro, https://www.nagarro.com/en, from offshore premises in India.

  Nagarro is accredited with Standards include CMMI, ISO 27001:2013, ISO 9001:2015, and ISAE 3402.