Yarris Technologies: Our commitment to security

Your partners in security

Yarris Technologies designs its processes and procedures to ensure commitment to information security objectives. Those objectives are based on the service commitments that Yarris makes to our clients, the laws and regulations that govern the provision of our services, and the financial, operational, and compliance requirements established for the services.

Yarris commitment to security is evidenced through the recent certifications of our Information Security Management System (ISMS) for ISO 27001 and SOC2. Regular third party audits and certification of our practices provides confidence and assurance that client data is being handled responsibly and securely.

Yarris Technologies operates as a security partner. Sometimes that means seamlessly integrating with our ISMS team. Sometimes that means serving as a security advisor for our customers that might be so focused on core competencies that they require a nudge and guidance toward ensuring the security of their internal data, as well as the personally identifiable information (PII) of their customers.

About our information security programs

As part of our commitment to security, Yarris Technologies adheres to a number of security standards and regulations, including:

ISO:27001

ISO:27001 provides requirements for an ISMS, using them enables organizations of any kind to manage the security of assets such as financial information, intellectual property, employee details or information entrusted by third parties.

The ISMS program covers:

- Access control
- Asset management
- Audit and compliance
- Data security
- Business continuity
- Information and communication
- Organization and management
- Risk management
- Software development lifecycle security
- Security operations

ISO 27001 CERTIFIED

A-LIGN

SOC 2

Developed by the American Institute of Certified Public Accountants (AICPA), SOC 2 is specifically designed for service providers storing customer data in the cloud, focusing on infrastructure and practices across areas representing its five Trust Service Principles: Security, Availability, Processing Integrity, Confidentiality and Privacy.

The SOC 2 program covers:

- Information during its collection or creation, use, processing, transmission, and storage
- Systems that use electronic information to process, transmit or transfer, and store information to enable the entity to meet its objectives.
- Controls over security prevent or detect the breakdown and circumvention of segregation of duties, system failure, incorrect processing, theft or other unauthorized removal of information or system resources, misuse of software, and improper access to or use of, alteration, destruction, or disclosure of information.

Exhaustive SOC 2 audits are repeated annually, and are authorised by an independent firm.