TMS SECURITY

Protecting your transportation network at every layer

Infios takes a proactive approach to TMS security—protecting your data, operations and reputation with built-in controls that evolve with the threat landscape.

infios
a Körber company

Infios has implemented a comprehensive information security program that integrates policies and procedures with both physical and logical security controls. Our program is aligned with the ISO 27001:2022 security controls framework.

Security practices
Our systems are hosted on industry-leading platforms, including the world's top cloud provider, to ensure maximum security, reliability and availability.

All hosting providers undergo annual audits and comply with key standards, including:

- SOC1 Type 2 and SOC2 Type 2
- GLBA and HIPAA
- TAR

Production environments are physically and logically separated from development environments. The network is protected by:

- Multi-protocol firewalls
- Restrictive, minimal rule sets
- Intrusion detection systems
- IP-based access restrictions

Our security program follows a multilayered, risk-based approach to protect customer data and assets. This includes:

- Industry-leading endpoint protection powered by artificial intelligence (AI) and machine learning (ML) to defend against zero-day threats.
- Best-in-breed cloud security tools
- Static, dynamic and manual application security testing
- A global, 24/7/365 security operations center (SOC) providing around-the-clock coverage

Application security
Application security is prioritized throughout the development lifecycle and beyond.

- Secure coding best practices are followed during development to ensure engineers consistently implement secure code all Infios IT systems and applications.
- Practices against sophisticated attacks is built in through techniques such as prepared statements to prevent SQL injection and cross-site scripting (XSS).
- Logical data segregation ensures each customer's data is separated within the application and database.
- Application-layer access only—direct database access is not permitted, further strengthening data security
- Role-based access control is enforced through Infios's hierarchical permissions model.
  - Users at the top of the hierarchy can configure visibility downward.
  - Users at lower levels only see data relevant to their corresponding level.
- Group, user, role and data-level permissions are fully managed by the customer's system administrator or super user.
- Granular permission structures ensure users and partners only access the data necessary for their role.

Highlights:

- ISO27001: internationally recognized standard with independent accreditation
- SOC1 Type 2 and SOC2 Type 2: independently verified security controls
- Security best practices across people, processes and technology
- Robust application security
- Rigorous operational security
- Proactive, prevention-focused security posture

Operational security
Our team continuously monitors emerging security threats and implements countermeasures to help prevent unauthorized access or unplanned system downtime. In addition to other security measures, we take the following steps:

- The dedicated security team actively evaluates threats and deploys updated countermeasures as needed.
- Endpoint protection is required on all servers and end-user devices to defend against viruses, malware, ransomware and other threats.
- Servers are isolated from direct internet access and are protected by multiple boundary defense layers, including firewalls and intrusion detection systems (IDS).
- Industry-standard security best practices are enforced across all infrastructure, including cloud-based systems, using defined hardening guides for every system build.
- System-wide monitoring enables rapid detection, response and containment of security incidents.
- Log aggregation and correlation—network, server, endpoint and associated security applications (e.g., antivirus) are sent to security information and event management (SIEM) and IDS for centralized monitoring.
- 24/7/365 incident detection and response system actively monitors all environments for malicious activity, indicators of compromise (IOCs) and suspicious behavior to ensure proactive threat response.

Proactive security measures
To ensure ongoing protection against emerging threats, we use a range of security testing tools to identify and remediate vulnerabilities in a timely manner. Our proactive measures include:

- Ongoing static and dynamic scans of the codebase and applications to detect potential security vulnerabilities.
- Regular system-level vulnerability scans to identify and address infrastructure threats.
- Cloud security tools and scans to assess and maintain the security posture of all cloud-based environments.
- Independent application penetration testing conducted by a third-party vendor.
- Internal and external penetration testing, also performed by an independent third-party vendor.

ABOUT INFIOS

Infios is a global leader in supply chain execution, relentlessly making supply chains better—every single day. With a portfolio of adaptable solutions, we empower businesses of all sizes to simplify operations, optimize efficiency and drive measurable impact.

Serving more than 5,000 customers across 70 countries, Infios delivers innovative technologies that evolve with changing business needs. Our deep expertise and commitment to purposeful innovation help businesses turn their supply chains into a competitive advantage—building resilience and shaping a more sustainable future.

Infios is a joint venture between international technology provider Körber and global investment firm KKR.

Ready for a supply chain that works relentlessly for you?

Connect with us to start your journey—no matter your industry, size or complexity, we're built to scale with you.

CONTACT US

infios
a Körber company

Infios.com