PUBLIC SECURITY OVERVIEW

TEMS CLOUD

Contents

1. Our Commitment to Security

At Infovista, security is a core principle of how we design, build, and operate TEMS Cloud. We understand that our customers rely on our solutions to handle critical data, and we take this responsibility seriously. Our approach to cloud security focuses on three pillars: protecting data, ensuring trust, and delivering reliability.

TEMS Cloud leverages Infovista's decades of experience in telecom-grade systems, combined with modern cloud security practices, to provide a secure and compliant platform for network testing, analytics, and optimization. Our security posture is continually reviewed and improved to meet evolving threats and compliance expectations.

This Security Overview outlines the measures, practices, and principles we follow to protect your data, ensure service availability, and maintain the integrity of our platform. We are committed to transparency, so you know exactly how we approach security and what steps we take to stay ahead of evolving threats.

Our security program is guided by internationally recognized standards and frameworks, including ISO/IEC 27001 – Information Security Management Systems (ISMS) certified, SOC 2 criteria (aligned), GDPR & CCPA – Data protection regulations for the EU and California, NIST Cybersecurity Framework (CSF), NIS2 Directive, EU Cyber Resilience Act (CRA) & EU Cloud Security Framework – Best practices and European regulations and initiatives designed to enhance cybersecurity resilience, product security, and cloud service trustworthiness.

By aligning with these standards, we ensure our security approach is comprehensive, globally relevant, and adapted to the specific challenges of telecom and cloud-based environments. We continuously monitor, test, and improve our systems to provide a secure, reliable, and resilient environment for your business.

Security is a shared responsibility — and together, we can ensure the confidentiality, integrity, and availability of your information.

2. Infrastructure & Network security

Hosting & Regions
TEMS Cloud is hosted on leading hyperscale cloud infrastructure with multiple, geographically distributed availability zones to ensure high availability, resilience, and performance. Customer environments are deployed in regional data centers that meet applicable data-residency and latency requirements.

Physical Security
All data centers used by TEMS Cloud implement multilayer physical and environmental protections, 24/7 monitored security operations, and independent audits. Facilities comply with internationally recognized standards such as ISO/IEC 27001 and SOC 2.

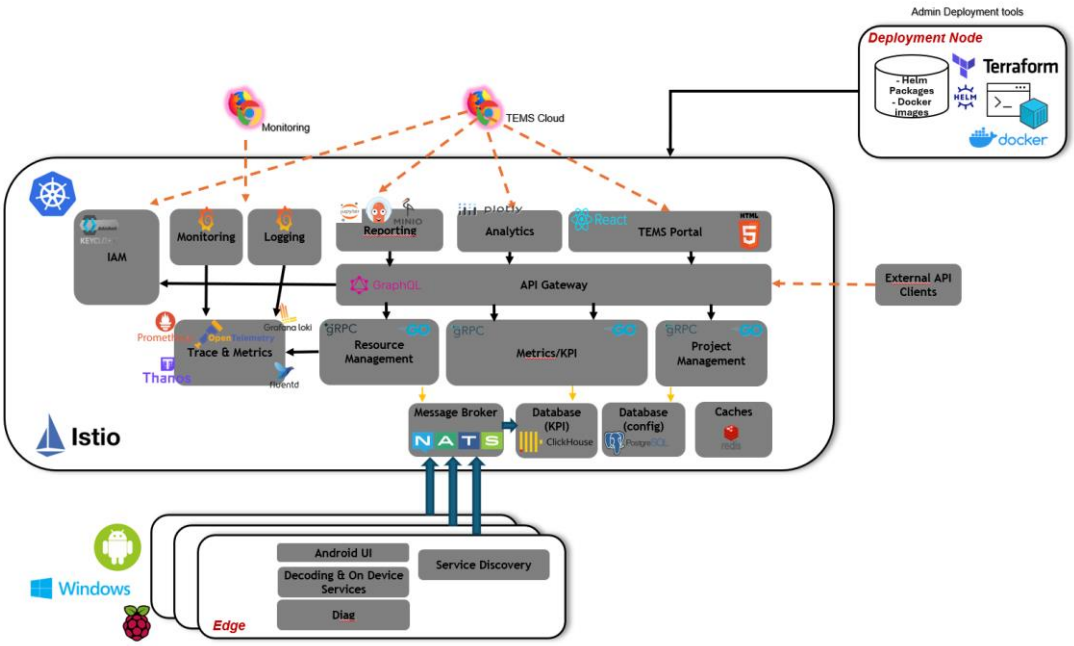
Network Security & Segmentation
TEMS Cloud employs a defense-in-depth network design, including secure HTTPS ingress, strict firewall policies, and segmentation between public and internal systems. Service-to-service communication is restricted by policy, and production, staging, and testing environments are fully isolated.

Perimeter Protection
Managed DDoS protection, rate limiting, and hardened edge gateways safeguard the service from external threats. All inbound traffic uses encrypted HTTPS/TLS connections, and outbound communications are restricted to authorized services.

Administration & Access Control
Administrative access is tightly controlled using multi-factor authentication (MFA), role-based access control (RBAC), and just-in-time privilege elevation. Infrastructure management follows automated and auditable configuration processes to ensure consistency and traceability.

Monitoring & Vulnerability Management
Continuous monitoring and centralized logging detect and alert on security-relevant events across applications, APIs, and infrastructure. Automated vulnerability scanning is integrated throughout the development and runtime environments to maintain a strong security posture.

Resilience & Recovery
High-availability and auto-healing mechanisms ensure service continuity. Encrypted backups are performed regularly and tested to validate recovery capabilities, supported by documented and periodically reviewed disaster-recovery procedures.



3. Data Protection and Privacy

Data Protection

TEMS Cloud applies comprehensive measures to safeguard customer data throughout its entire lifecycle — from collection and storage to retention and deletion — in alignment with global privacy and security standards.

Data Classification & Minimization
All data is classified according to sensitivity (e.g., internal, customer, confidential) and handled under defined protection rules. TEMS Cloud follows a strict data minimization approach, ensuring that only the information necessary for service operation is processed. Non-production environments use synthetic or anonymized data.

Encryption & Key Management
Customer data is protected using strong encryption — in transit via HTTPS/TLS and at rest using industry-standard algorithms. Encryption keys are securely managed through controlled key management systems with enforced access control, rotation, and revocation procedures.

Retention & Disposal
Data is retained only for as long as required to meet contractual, operational, or legal obligations, after which it is securely deleted or anonymized in accordance with corporate policy. Customers may request data export or deletion in compliance with applicable data protection laws, such as GDPR.

Data Residency
Customer environments are hosted in regional data centers chosen to meet data-residency and performance requirements. Data remains within the designated region unless otherwise agreed for disaster recovery or specific contractual needs.

4. Identity & Access Management

User identity and access management are critical to maintaining the integrity of TEMS Cloud. Infovista enforces a defense-in-depth approach to managing identities and controlling access to systems and data within the TEMS Cloud platform.

Authentication & Authorization
Access to TEMS Cloud services is protected through strong authentication mechanisms, including multi-factor authentication (MFA) and single sign-on (SSO) integration. Role-based access control (RBAC) ensures users are granted the minimum privileges necessary to perform their duties, following the principle of least privilege.

Administrative Access Controls
Administrative accounts are tightly restricted, monitored, and reviewed periodically. All privileged operations require MFA and are limited to trusted networks or managed devices. Temporary, just-in-time access is used when elevated permissions are needed for maintenance or incident response.

Account Provisioning & Lifecycle Management
User accounts are created, modified, and deactivated through controlled workflows that enforce approval and traceability. Access reviews are conducted on a regular schedule to verify that permissions remain appropriate.

Monitoring & Audit Logging
Access to sensitive systems and data is continuously logged and monitored. Security operations teams review audit logs and alerts to detect unauthorized or anomalous access attempts.

Customer Integration & Responsibility
Customers can integrate their corporate identity providers via SSO to align authentication with their internal security policies. Each customer remains responsible for managing user access within their tenant environment, while Infovista maintains platform-level identity and access controls.

5. Application & Development Security

Security is integrated into every stage of the TEMS Cloud software development lifecycle — from initial requirements and design to deployment and ongoing operations — ensuring that controls are preventive by design and continuously validated.

Secure Software Development Lifecycle (SDLC)
Infovista follows a structured and secure development process that incorporates security requirements, design reviews, secure coding standards, automated code analysis, and independent security testing. Each product release must complete a formal security review and sign-off prior to deployment.

Secure Coding & Review Practices
Development teams follow recognized secure-coding frameworks such as OWASP, supported by automated scanning and peer code reviews. All identified security issues are assessed for risk and remediated according to defined priorities and timelines.

Vulnerability & Dependency Management
Automated tools continuously scan application code and third-party components to detect vulnerabilities. Identified issues are tracked to closure, and all high-risk findings are addressed before production release. Software Bills of Materials (SBOMs) are maintained to ensure transparency and support supply-chain integrity.

Testing & Quality Assurance
Each release undergoes comprehensive security testing, including automated vulnerability scans, code analysis, and targeted penetration tests. The testing process follows recognized industry standards and best practices to validate the platform's resilience.

Change & Release Governance
All changes to the TEMS Cloud application follow formal change-management procedures.

Security gates are embedded within the build and deployment pipelines, ensuring that only validated, approved, and securely configured releases are promoted to production

6. Monitoring & Threat Detection

TEMS Cloud is continuously monitored across all layers of its infrastructure and application stack to detect and respond to potential threats in real time.

Continuous Monitoring
Infovista maintains centralized monitoring and logging across application, platform, and identity services. Security events and system metrics are collected, correlated, and analyzed to identify anomalies, policy violations, and potential indicators of compromise.

Threat Detection & Analysis
Advanced detection mechanisms combine rule-based alerts with behavioral analytics to identify suspicious activity or deviations from normal patterns. Monitoring extends to authentication events, access changes, configuration integrity, and network behaviors to ensure early detection of potential threats.

Incident Response & Escalation
Detected threats are automatically routed to security operations teams for triage, investigation, and remediation. High-severity alerts trigger immediate escalation under Infovista's documented incident response procedures. Post-incident reviews are conducted to identify root causes and strengthen preventive controls.

Customer Notification
In the event of an incident that could impact customer data or service availability, Infovista promptly informs affected customers in accordance with its incident communication policy and applicable legal or contractual requirements.

7. Compliance & Certifications

TEMS SaaS is certified to the **ISO/IEC 27001** standard, the globally recognized framework for managing information security. This certification demonstrates Infovista's commitment to protecting customer data through robust, risk-based controls and continuous improvement within our Information Security Management System (ISMS).

While ISO/IEC 27001 serves as our formally certified framework, TEMS SaaS also operates in alignment with other major international standards and regulations, including the **EU General Data Protection Regulation (GDPR)** and the **California Consumer Privacy Act (CCPA)**.

Our security and privacy controls are independently audited by third parties each year to validate their effectiveness and ensure ongoing compliance. Certification renewals are performed annually, and summary attestations can be provided upon request.

Where required and agreed in advance, TEMS SaaS may support **customer-initiated security or compliance assessments**, coordinated under mutually approved scope, methodology, and confidentiality agreements.

8. Incident Management and Response

Despite best efforts, no system can be entirely immune to security incidents. Infovista maintains a structured incident response process designed to detect, contain, and remediate security issues quickly and effectively.

In the event of a security incident affecting customer data or service availability, customers will be notified promptly through established communication channels. Transparency and collaboration are key to our approach — our goal is to restore full service quickly while keeping customers informed throughout the process.

9. Business Continuity and Resilience

TEMS Cloud has been designed for high availability and operational resilience. Redundant infrastructure, regular backup processes, and tested disaster recovery procedures ensure that customer data remains protected and services continue to operate even in adverse conditions.

Our continuity planning is periodically reviewed and validated through simulations and tests to ensure readiness for unexpected events. The outcome is a service that customers can rely on for critical business operations.

Our goal is simple: to earn and maintain the trust of our customers by delivering a platform that is secure, reliable, and transparent.

10. Customer Responsibilities

Security in the cloud is a **shared responsibility** between Infovista and its customers. While Infovista manages the security of the infrastructure, platform, and application layers, customers are responsible for securing how they configure, access, and use their own environments within **TEMS Cloud SaaS**.

Customer Responsibilities Include:

Password Management
Customers are responsible for maintaining the confidentiality and integrity of their login credentials. This includes creating strong, unique passwords, storing them securely (e.g., in

password managers), avoiding reuse across systems, and changing them promptly if compromise is suspected.

Session Security
Users must manage active sessions securely by logging out when leaving devices unattended, avoiding the use of "remember me" features on shared devices, and locking screens when not in use.

Data Classification & Input Controls
Customers are responsible for ensuring that any data uploaded to TEMS Cloud complies with their own organizational and regulatory obligations. TEMS Cloud does not process personally identifiable information (PII) unless explicitly agreed under a **Data Processing Agreement (DPA)**.

Endpoint Security
Customers should protect the devices and networks used to access TEMS Cloud by maintaining up-to-date software, enabling antivirus/anti-malware protection, and avoiding untrusted or public networks when handling sensitive information.

Incident Reporting
Customers must promptly notify Infovista of any suspected compromise, misuse, or unauthorized access to their TEMS Cloud environment.

What Infovista Manages:

- **Infrastructure Security** – Physical and network protections, including firewalls, intrusion detection/prevention systems, and segmentation.
- **Application Security** – Secure coding, vulnerability management, patching, and penetration testing of the TEMS Cloud application.
- **Availability & Resilience** – Disaster recovery, data backup, and redundancy to ensure service continuity.
- **Compliance & Certification** – Maintenance of ISO/IEC 27001 certification and alignment with GDPR, CCPA, and other regulatory frameworks.

11. Continuous Improvement and Trust

Security is not a one-time effort but an ongoing commitment. Infovista continually evaluates new threats, regulatory developments, and customer expectations to enhance the TEMS Cloud security posture. Training, awareness programs, and close collaboration between engineering and security teams ensure that best practices are consistently applied.

12. Security Contact & Reporting

Provide reporting channels and how to contact in case of a security incident.

As a customer of TEMS Cloud, we want to ensure you get the best possible support experience. That is the reason why all support requests should be submitted through our **Infovista Support Portal.**

To submit a request, simply log in to the Support Portal and open a ticket (Registration required). Our team will assist you as quickly as possible.

How to Register for the Support Portal

As a new TEMS Cloud customer, you will need to register on our support portal to access assistance and resources. Please follow the steps below to create your account:

1. **Go to** Infovista Support Portal
2. **Click on** *Customer Login*.
3. **Select** *Not a member?* to begin the registration process.
4. **Complete the registration form** and ensure you select **"TEMS"** as your product line.
5. **Submit the form** to finalize your registration.
6. Once submitted, you will receive an email with your user account details, allowing you to access the Infovista portal

In the event of a security incident, TEMS follows a four-phase approach: Detect, Respond, Remediate, Recover. Customers are notified within 24 hours of confirmed incidents, and a full incident report is shared within 5 business days

A root cause analysis and mitigation plan are provided within 7 business days for incidents categorized as High or very high impact.

13. Summary

TEMS Cloud combines Infovista's long-standing expertise in telecom and software development with a robust, modern approach to cloud security. From secure infrastructure to responsible data management, every element of the service is designed to protect customer information and ensure operational confidence.

By continuously investing in security, compliance, and resilience, Infovista ensures that TEMS Cloud remains a trusted platform for customers around the world.