KENEXIS

Kenexis Integrated Safety Suite

SECURITY WHITE PAPER

ISO 27001 - Aligned Security for the Process Industries

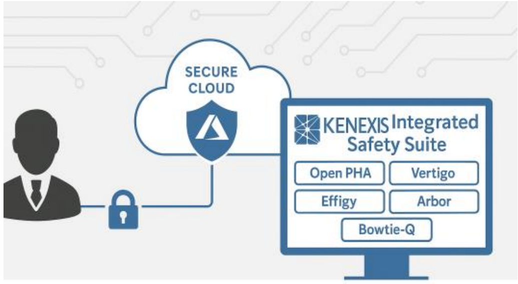
ISO 27001 - Aligned Security for the Process Industries

Kenexis Consulting Corporation
www.kenexis.com

1. Introduction and Overview

At Kenexis Consulting Corporation, security is more than a compliance exercise — it is the foundation of trust with our clients in the process industries. Our **Kenexis Integrated Safety Suite (KISS)** is a cloud-based SaaS platform designed for enterprise safety and risk management. Because our customers depend on us to safeguard critical industrial safety data, we have built our platform to conform with the rigorous international standard **ISO/IEC 27001** for information security management.

Kenexis Integrated Safety Suite (KISS) is a comprehensive cloud-based SaaS platform designed to support technical safety activities across the process industries. It brings together a suite of specialized tools—such as Open PHA for process hazard analysis, Vertigo for safety instrumented systems, Effigy for fire and gas mapping, Arbor for fault tree analysis, and Bowtie-Q for barrier risk management—into a unified environment. By integrating these applications, KISS enables organizations to efficiently manage safety lifecycle data, perform advanced risk analysis, and ensure compliance with regulatory and industry standards, all while reducing duplication of effort and improving collaboration across teams.



Kenexis Integrated Safety Suite

The platform is securely deployed through Microsoft Azure, leveraging the scalability, resilience, and global reach of Microsoft's enterprise-grade cloud infrastructure. Azure provides the underlying security, data redundancy, and compliance frameworks that support Kenexis' ISO 27001–aligned Information Security Management System. Customers benefit from high availability, encrypted data storage and transmission, and seamless integration with enterprise IT systems, while Kenexis ensures that security controls and policies are consistently implemented across the entire platform. This deployment model allows clients to access powerful safety and risk management tools from anywhere while maintaining confidence in the security and integrity of their data.

This whitepaper provides an overview of how we secure our platform, the frameworks we follow, and the practices we embed in our daily operations.

2. Commitment to ISO 27001

Kenexis has achieved conformance with **ISO 27001**, the globally recognized benchmark for information security management systems (ISMS). This standard requires us to identify, assess, and mitigate security risks across all areas of our operations.

- **Policy Framework**: Comprehensive information security policies, reviewed annually, guide our organization.
- **Management Oversight**: Our executive leadership, including the Technical Director, actively participates in risk management and annual reviews.
- **Continuous Improvement**: Our ISMS is a living system, with regular audits, reviews, and corrective actions driving improvements.

Within the **Kenexis Integrated Safety Suite**, these ISO 27001 principles are embedded into the way the platform is built and maintained. Each module of the suite—whether Open PHA, Vertigo, Effigy, Arbor, or Bowtie-Q—is governed by strict access controls, encryption standards, and monitoring practices that align with the ISMS. Development processes follow secure coding standards, while deployment through Microsoft Azure ensures system resilience, redundancy, and compliance with international security standards. By combining our organizational policies with platform-level safeguards, Kenexis delivers not only regulatory alignment but also a strong, practical assurance that client safety and risk data remains secure, confidential, and available.

3. Governance & Organization

We maintain a clear organizational structure for security responsibilities:

- **Defined Roles & Responsibilities** – Security roles are documented in our ISMS plan and role descriptions.
- **Separation of Duties** – Access rights and responsibilities are periodically reviewed to avoid conflicts of interest.
- **Engagement with Authorities & Industry** – We maintain appropriate contacts with regulators, standards groups, and industry associations.

This ensures that information security is embedded in every project that impacts our SaaS platform.

This structured approach to governance strengthens the overall security posture of the **Kenexis Integrated Safety Suite** by ensuring accountability and oversight at every level of the organization. With security responsibilities clearly defined, issues can be escalated and resolved quickly, reducing the likelihood of vulnerabilities going unnoticed. The periodic review of access rights ensures that only authorized personnel have entry to sensitive systems, minimizing insider risk and enhancing compliance with regulatory requirements. Moreover, active participation in industry forums and engagement with authorities allows Kenexis to stay ahead of evolving security threats and regulatory changes, incorporating best practices and lessons learned directly into the platform. This combination of internal rigor and external awareness ensures that governance is not a static function, but a dynamic force that continuously improves the resilience and reliability of the Kenexis Integrated Safety Suite.

4. Technical Security Controls

Kenexis employs a multi-layered defense strategy aligned with ISO 27001 Annex A controls:

- **Secure Development & Operations** – All projects that impact the SaaS platform are tracked in **Azure DevOps**, with security requirements integrated from the outset.
- **Access Management** – User access to sensitive systems and client data is reviewed regularly, with strict authentication and authorization mechanisms.
- **Mobile & Remote Work Security** – Company-issued and personal devices are governed by policies covering encryption, VPN access, and remote security standards.
- **Cloud Infrastructure** – Our platform leverages hardened cloud services with continuous monitoring, logging, and incident detection capabilities.

These layered technical safeguards work together to create a resilient and adaptive security environment for the **Kenexis Integrated Safety Suite**. By embedding security into both the software development lifecycle and daily operations, Kenexis ensures that vulnerabilities are identified early, access is strictly controlled, and potential threats are continuously monitored. The combination of proactive measures, such as secure coding and device policies, with reactive capabilities, like real-time incident detection and response, allows the platform to address both known risks and emerging cyber threats. This holistic approach not only aligns with ISO 27001 Annex A requirements but also provides clients with confidence that their critical safety and risk management data is protected by enterprise-grade security at every layer.

5. Data Protection & Privacy

We treat customer data with the highest sensitivity.

- **Privacy Policy** – Kenexis enforces a published **Data Protection and Privacy Policy** that governs handling of client information.
- **Encryption** – All data is encrypted both at rest and in transit using industry-standard protocols.
- **Backup & Continuity** – Data is regularly backed up with tested recovery procedures to ensure availability even in the event of disruption.

Beyond these core measures, **Kenexis Integrated Safety Suite** incorporates strict data segregation and role-based access controls to ensure that each client's information remains fully isolated and accessible only to authorized users. Comprehensive audit logging provides visibility into all access and activity, allowing Kenexis to monitor compliance with security and privacy requirements. In addition, Kenexis continuously evaluates evolving data protection regulations, such as GDPR and other regional standards, and adapts its policies and controls accordingly. This proactive stance not only safeguards sensitive safety and risk management data but also ensures that customers can demonstrate compliance with global privacy expectations when using the platform.

6. Human Resources Security

People are at the center of security.

- **Pre-employment Screening** – Employees and contractors undergo security vetting prior to hiring.
- **Training & Awareness** – Ongoing training ensures that staff understand their responsibilities in safeguarding client data.
- **Confidentiality Agreements** – Employees formally acknowledge confidentiality obligations as part of their contracts.

Kenexis further reinforces its human resources security by cultivating a culture of accountability and vigilance across the organization. Security expectations are woven into performance reviews, project management practices, and day-to-day operations, ensuring that data protection is treated as a shared responsibility rather than a standalone task. By combining upfront vetting with continuous education and contractual commitments, Kenexis ensures that every individual involved in delivering and supporting the **Kenexis Integrated Safety Suite** contributes actively to maintaining the confidentiality, integrity, and availability of client data.

7. Continuous Improvement & Assurance

Security is not a one-time achievement.

- **Internal Audits** – Regular audits measure performance of the ISMS against ISO 27001 requirements.
- **Management Reviews** – Annual reviews ensure alignment with evolving risks, business needs, and regulatory changes.
- **Corrective Actions** – Identified gaps are addressed promptly with formal remediation plans.

For the **Kenexis Integrated Safety Suite**, continuous improvement also extends into the lifecycle of the platform itself, where security practices evolve alongside product development and client usage patterns. Feedback from audits, reviews, and client interactions is incorporated into the development roadmap, ensuring that both technical features and security safeguards advance in parallel. Threat intelligence and lessons learned from industry incidents are regularly evaluated and used to update policies, procedures, and technical defenses. This proactive approach means that Kenexis is not only responding to identified issues but also anticipating emerging risks, keeping the platform resilient and reliable as security challenges and regulatory expectations change over time.

8. Conclusion

The **Kenexis Integrated Safety Suite** is built to the highest standards of security, giving process industry organizations confidence that their safety and risk management data are protected. Our ISO 27001 alignment demonstrates not only compliance, but also our deep commitment to safeguarding the integrity, confidentiality, and availability of client information.

Security is built into everything we do — from the way we develop our software, to how we train our people, to how we continuously improve.