Protecting industrial information is fundamental to how we operate.

At Gizil, information security is an integral part of how we develop, operate and support Virtual Plant®, our industrial spatial digitalization platform, and deliver related services.

We recognize the sensitivity of industrial facility information, including engineering documentation, asset data, point clouds and operational records. Our approach is designed to protect this information while enabling authorized teams to access and use it effectively.

Our Commitments

Confidentiality and Data Protection

We protect customer and company information through appropriate access controls, confidentiality obligations and secure information-handling practices. Customer information is accessed only for authorized business and service purposes.

Secure Platform Operations

Information security is considered throughout the development, deployment, operation and maintenance of Virtual Plant. We apply risk-based security measures to protect the confidentiality, integrity and availability of information.

Risk Management and Business Continuity

We identify and assess information security risks, including relevant technology dependencies and service disruptions. Business continuity and incident response arrangements support the resilience of critical operations.

People and Third-Party Security

Our personnel are required to follow information security and confidentiality obligations. External service providers are assessed and managed according to their responsibilities, access to information and associated risks.

Compliance and Continual Improvement

We are committed to meeting applicable legal, regulatory and contractual information security requirements. We monitor security performance, review incidents and risks, and continually improve our information security practices.

Printed copies are uncontrolled unless verified against the current electronic version.
© Gizil. All rights reserved.

Our Management Framework

Gizil maintains an Integrated Management System incorporating quality, occupational health and safety, and information security, aligned with ISO 9001, SCC and ISO/IEC 27001:2022.

Our information security practices are governed by documented policies, assigned responsibilities, risk assessments and management oversight.

For customer-specific security requirements, deployment arrangements or information security inquiries, please contact info@gizil.de.

Esma Gulten
Managing Director
Gizil

Printed copies are uncontrolled unless verified against the current electronic version.
© Gizil. All rights reserved.