Cloud Security Overview

toolsgroup

Index

Executive Summary:

An Introduction to ToolsGroup's Approach to Information Security

ToolsGroup puts customers first.
A critical part of delivering our promises to customers is safeguarding customer data with a comprehensive, multi-layered security program. This document outlines our cloud security measures, regulatory compliance and operational practices designed to protect data in ToolsGroup Cloud. We continuously benchmark against the highest industry security standards, integrating robust vulnerability management and active threat monitoring to proactively adapt our defenses to emerging threats.

Security isn't just a checkbox for us. It's an integral part of our solutions and operations, enabling continuous improvements to keep your data safe.

+ Architecture Overview

ToolsGroup delivers modern supply chain solutions as Software as a Service (SaaS). We rely on world-class cloud providers and hyperscalers to deliver our infrastructure, ensuring high performance, seamless scalability and robust security. By utilizing the global data center networks of these leading platforms, we bring the solution closer to users around the world— supporting data residency requirements and minimizing latency. This approach enables us to deliver a resilient, secure, and highly responsive service experience.

Security by Design

From the ground up, the ToolsGroup cloud solution employs multiple layers of security to protect customer applications and data:

Strong user authentication

Rigorous access controls

Data encryption

Continuous vulnerability scanning

Audited operational processes

Many other security features, evolving constantly to ensure our solutions have industry-leading information protection

Security is built into every layer of our architecture and processes, not added as an afterthought.

+ Data Security

Data Centers and Physical Security

Data Centers and Physical Security

ToolsGroup's SaaS offering is hosted on Tier 3+ data centers provided by world-class providers. These facilities maintain strict physical security controls to prevent unauthorized access to servers and storage. They use multi-layered security perimeters, biometric and card access systems, 24/7 guarded surveillance, and continuous video monitoring to prevent unauthorized personnel. Regular independent audits and assessments are conducted to ensure the facilities adhere to stringent security requirements and evolving best practices.

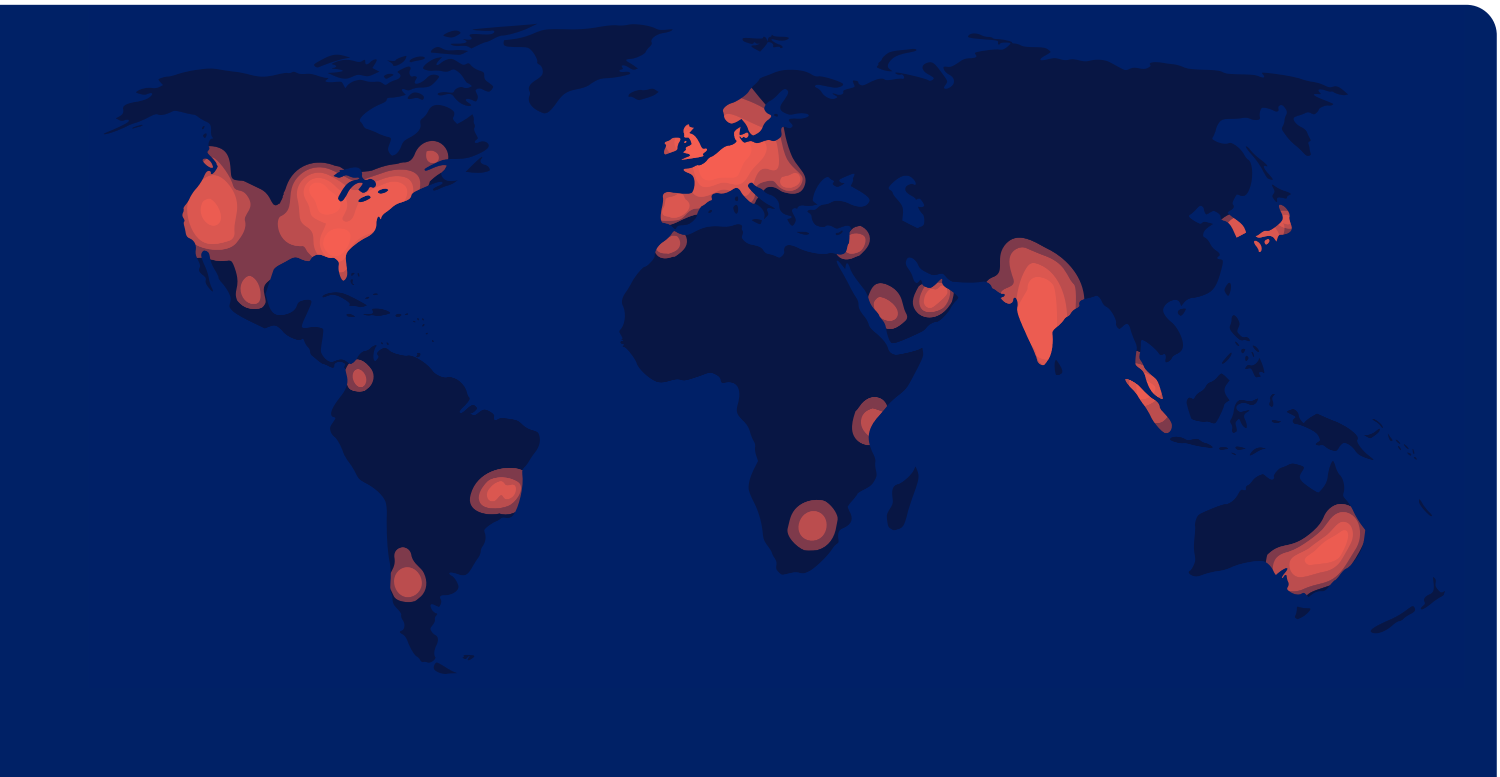
Data Residency

The global presence of our cloud providers' data centers allows ToolsGroup to deploy your solution in a region that meets your data residency needs and optimizes performance for your users. Our providers operate dozens of regions worldwide, each engineered with redundant power, cooling, and networking, so your data is stored in secure, highly available environments designed to withstand failures and natural disasters. This geographic diversity, combined with careful region selection, helps us comply with local regulations and keep your data close to home.

Partner Certification and Compliance

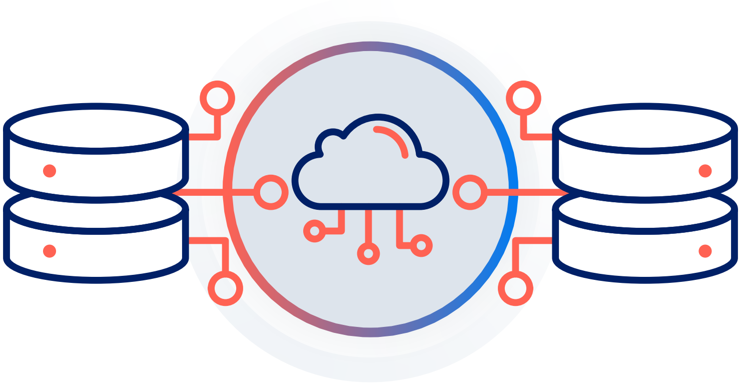
Our cloud platform partners are certified against a broad set of industry and government security standards. The underlying infrastructure meets international and regional compliance benchmarks such as ISO/IEC 27001, SOC 1/2/3, FedRAMP, and others. It also adheres to data privacy requirements in various jurisdictions, including EU General Data Protection Regulation (GDPR) and standard contractual clauses for cross-border data transfer. By building on a compliant cloud foundation, ToolsGroup ensures that the physical and environmental security, as well as baseline compliance, are of the highest standard from the start.

Regions with Data Centers



Service Resilience and Data Redundancy

To safeguard availability, ToolsGroup employs robust service redundancy at multiple levels. Any data stored in our solution is kept in redundant copies within the primary hosting region, and it is also asynchronously replicated to a geographically separate secondary region. This geo-redundancy means that even if an entire data center region faces an outage, an up-to-date copy of your data remains available in the backup region, minimizing risk of data loss. The secondary region is carefully chosen to be an appropriate pair for the primary region, balancing distance as well as regulatory requirements.



High Availability

The application's supporting infrastructure is built with no single points of failure. Redundant instances, load-balanced services, clustered databases, and network failover mechanisms are in place to ensure continuous operation even if individual components fail. Our cloud architecture inherently provides high availability for critical components, and we back this with a financially guaranteed Service Level Agreement (SLA).

Disaster Recovery

ToolsGroup has a documented disaster recovery plan that is tested regularly. In the event of a major outage affecting the primary environment, we can fail over to the secondary region to restore service quickly. We commit to an aggressive Recovery Point Objective (RPO) and Recovery Time Objective (RTO) of 24 hours for our cloud service. In other words, in the worst cases, up to 24 hours of data might be lost (RPO) and service should be restored within 24 hours (RTO) after a catastrophic event. We aim to recover much faster. These recovery objectives are included in our standard SLA for all customers.

Data Backups

ToolsGroup performs regular backups of the entire system. We take full snapshots of critical virtual machines and databases on a daily basis and retain these backups for a rolling period of 15 days to offer point-in-time recovery options. Backup data is stored encrypted and in a geo-redundant manner, separate from the live data, to protect against catastrophic loss. In summary, your data has multiple layers of protection: real-time replication to a secondary site and offline backups in secure storage.

Data Security and Privacy

Customer Data Ownership

ToolsGroup recognizes that your data is your property. Thw customer is the exclusive owner of all data put into our solution. We act as a steward of that data, processing and storing it only to fulfill our service obligations. Our internal administrators (ToolsGroup operators) access customer data only when necessary to support your needs—such as resolving a support issue or performing maintenance— and only with proper authorization. Such access is limited to purposes that are compatible with providing the contracted services and subject to strict oversight.

We require the same commitments from any subcontractors we use. Third-party sub-processors can access customer data solely to perform the services they are engaged for, and nothing more. ToolsGroup maintains a transparent list of these sub-processors that is made available to customers and provides advance notice of any changes. You always know who might handle your information.

Data Isolation

Each customer's environment is completely segregated at the application and database level. Your data is stored in its own dedicated database/schema and never co-mingled with anyone else's data. This data isolation is a core benefit of our architecture. It prevents any possibility of one customer inadvertently accessing another's information and simplifies compliance with data segregation requirements.

Full Encryption, Everywhere

ToolsGroup employs strong encryption to protect customer data in all states: in transit, at rest, and in backups. All data transmitted to and from the application (for example, user traffic between your browser and our cloud) is encrypted in transit using TLS (Transport Layer Security).

We require modern cryptographic protocols and cipher suites. Our configurations are continually updated as new vulnerabilities emerge to meet or exceed industry standards for transport encryption. This includes enforcing a minimum of TLS 1.2 and using long key lengths for maximum protection.

Data "at rest" in the ToolsGroup Cloud (databases, storage, backup files, etc.) is also encrypted using strong algorithms (AES-256). Each customer's data encryption keys are managed by ToolsGroup in a secure key management system and are unique to that customer's environment. This means even if someone somehow obtained a disk image from our servers, the data would be unreadable without the proper keys. Backup files and replicas in secondary regions are likewise encrypted at rest. In short, all customer data is encrypted at rest and in transit by default, as a non-negotiable security measure.

Continuous Data Protection

In addition to encryption, ToolsGroup maintains rigorous processes for data integrity and availability. We monitor the cryptographic algorithms and protocols in use as part of our vulnerability management program, ensuring that we swiftly replace or upgrade anything that no longer meets current security guidelines. Through regular penetration tests and security assessments, we validate that customer data remains secure against the latest threats. All these measures work in concert to give you confidence that your sensitive information is safe with ToolsGroup.

+ Operational Security

Our operational security practices ensure that the platform is managed and maintained in a secure manner day-to-day. This covers how we size and scale the system, manage user access, monitor activities, and control changes.

Scalability and Performance

ToolsGroup's cloud solution is designed to scale to meet customer needs without compromising security. We offer standardized deployment tiers (Small, Medium, Large) that cover common workload profiles, and we can further scale resources on demand if your usage grows. Scaling is performed within a planned maintenance window, typically during off-hours, to minimize any business impact. Our team works with you to right-size the environment and can rapidly add capacity (CPU, memory, storage, etc.) whenever needed.

This flexible scaling ensures that performance and responsiveness remain optimal as your data volume or user count increases, while keeping the environment secure and stable. By aligning capacity with demand, we maintain strong performance and cost-efficiency, while avoiding any performance bottlenecks that could otherwise lead to security issues or downtime.

Federated Authentication and Single Sign-On (SSO)

To provide secure and convenient access for users, ToolsGroup supports federated authentication and Single Sign-On (SSO) integration with your identity systems. Federated SSO allows your users to log in to the ToolsGroup application using their existing corporate credentials, managed by your chosen Identity Provider (IdP), such as Azure Active Directory, Okta, PingIdentity, or others. We have implemented support for industry-standard SSO protocols, including SAML 2.0 (Security Assertion Markup Language) and OAuth 2.0 / OpenID Connect (OIDC), which are the same technologies used by leading SaaS providers for single sign-on. This means ToolsGroup can seamlessly integrate into your single sign-on environment. When users attempt to access our application, they will be redirected to your organization's central login page, and after successful authentication, including any required multi-factor authentication at your side, they gain access to our service without a separate login.

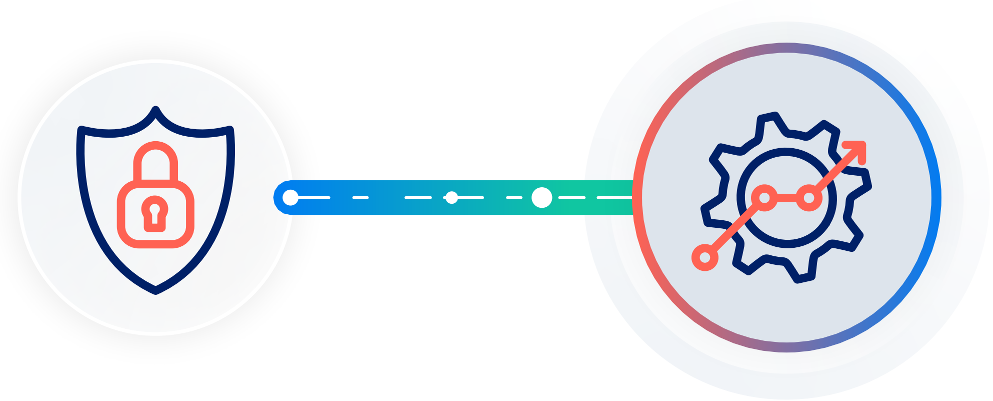
Capabilities

Our SSO integration supports service provider-initiated logins where users go to the ToolsGroup URL first and are then redirected to the IdP for authentication. We utilize secure federation standards, such as exchanging signed SAML assertions or OIDC tokens, to establish the user's identity and permissions in our application without ever storing your users' passwords in our systems. This approach enhances security by centralizing authentication with your IdP— credentials are **not duplicated**— and by allowing you to enforce your own password policies and multi-factor authentication (MFA) for ToolsGroup access just as you do for your other enterprise apps. ToolsGroup's platform is compatible with any SAML 2.0-compliant identity provider, and our team will provide guidance on configuration. (We have successfully integrated with Azure AD, ADFS, Okta, OneLogin, Auth0 and others in real-world customer deployments.)

Business Benefits

Enabling single sign-on with ToolsGroup has multiple advantages. User convenience is improved, as users have one fewer password to manage. They can access the system faster, which encourages adoption and reduces login-related support tickets. Centralized access control means that you can provision or revoke user access to ToolsGroup from your central directory. For example, when an employee leaves your company or changes roles, updating your directory automatically affects their ToolsGroup access. This greatly simplifies onboarding and offboarding processes and ensures that access rights stay in sync with your organization's current state.

Most importantly, SSO contributes to stronger security. You can apply uniform login policies, such as requiring MFA or session timeouts, to ToolsGroup via your IdP. This also reduces the risk of weak or reused passwords since users are not creating new credentials for each software. Federated SSO support in ToolsGroup provides enterprise-grade identity management integration, helping you streamline authentication while maintaining full control and visibility.



Alternative Authentication

For customers who prefer not to use SSO, ToolsGroup also offers a robust built-in authentication system. In such cases, we enforce strict password policies to protect accounts. Passwords must meet complexity requirements, such as minimum length of 8 characters including both uppercase and lowercase letters, at least one number, at least one special character, etc. Password reuse is prohibited, even partial reuse or simple variations on recent passwords, to ensure that new credentials are truly unique. After five consecutive failed login attempts, an account is automatically locked for 30 minutes as a protection against brute-force attacks. These measures align with industry best practices for password security.

Of course, we highly encourage use of SSO for the optimal combination of security and user experience. Regardless, if local accounts are used, they are defended with stringent controls.

Security Monitoring and Audit Logging

ToolsGroup maintains comprehensive logging and monitoring of the cloud environment to quickly detect suspicious activity or anomalies. All access to the Solution and key actions performed within it are logged centrally. This includes authentication attempts, user logins/logouts, administrative changes, and other security-relevant events. Logs from applications, underlying servers, network devices, and security systems all feed into a centralized Security Information and Event Management (SIEM) system.

The SIEM continuously analyzes log data and will generate automatic alerts to our security team if any activity falls outside of defined safe thresholds or matches known threat patterns. For example, the SIEM would alert on things like repeated failed logins, unusual after-hours access, sudden role changes, or anomalies in system performance that might signal an attack. This real-time monitoring allows ToolsGroup operators to respond rapidly to potential security issues— often before they impact customers.

Audit logs are retained in a tamper-resistant repository for an extended period (at least 180 days). These audit logs include records of security-related events such as login attempts, password changes, permission changes, and other administrative actions. Storing them in an inalterable form means we have a trustworthy history of events that can be examined during incident investigations or compliance audits. Customers can request reviews of relevant log data as needed for their own security audits. By retaining six months of history, as well as longer records in backups, we align with common compliance requirements and ensure traceability of actions in the system.

Our operations team uses an integrated monitoring system that keeps watch on the health and performance of all components of the solution— compute, storage, network, and application metrics. This goes beyond security events. It also tracks uptime, resource utilization, and error rates. If any metric— CPU spikes, memory leaks, slow response times, or unusual traffic patterns— goes out of normal range, our team is alerted. This comprehensive monitoring helps us detect not only security incidents but also any technical issues that could affect availability or performance, enabling a proactive response 24/7.

Change Management

ToolsGroup follows a strict change management process for any updates to the cloud environment. We understand that uncontrolled changes can introduce security risks or instability, so we've instituted formal procedures to manage changes safely. All changes, such as applying a software update, modifying network configurations, or adjusting infrastructure, must be requested and documented through our Ticketing Support Portal.

Each change request undergoes an impact assessment where our technical teams evaluate potential risks, including security implications and effects on other customers or components. Changes are reviewed and approved by authorized personnel before implementation. We schedule changes during maintenance windows and provide advance notice to customers for any major updates. Post-change, we perform testing and monitoring to ensure the change had the intended effect— and only the intended effect. This disciplined approach to change management is part of our ISO 27001 procedures and helps maintain the integrity, availability, and security of the service over time.

+ Secure Operations by ToolsGroup Personnel

Security isn't only about technology. It's also about the people who manage the technology. ToolsGroup ensures that our internal operations teams follow rigorous security practices when accessing and administering the cloud systems.

All ToolsGroup operators and engineers who manage the SaaS environment do so from secure, controlled locations. Access to management consoles and servers is done over encrypted channels, enforcing TLS for remote connections, and requires multi-factor authentication (MFA) for any sensitive administrative operations. This means that even if an admin's password were compromised, an attacker could not get into the system without the second authentication factor, which is typically a time-based one-time code or a hardware token possessed only by our staff. We log and audit all administrator actions for oversight.

Every ToolsGroup workstation and laptop used by our personnel is secured with full disk encryption, up-to-date endpoint protection, and configurations that comply with our corporate security policies, including regular patching and vulnerability scanning. Importantly, these workstations have no direct access to customer data. Administrative work is performed through intermediate jump hosts or management interfaces that separate our corporate network from customer environments. By implementing this separation, even a compromised employee device would not have a straightforward path to sensitive customer information.

We also maintain least-privilege access control. Our team members are granted only the minimum permissions they need to do their job. Within ToolsGroup, we assign clear security-related roles and responsibilities, including a dedicated Information Security Manager, security officers, etc., so there is proper oversight and accountability to protect customer data. Regular training is provided to all employees on security awareness, data handling, and incident response protocols.

ToolsGroup's own operations are secured through MFA, encryption, network isolation, and policy enforcement, ensuring that the people behind the service uphold the same high security standards used to secure your data.

+ Business Continuity and Disaster Recovery

ToolsGroup has extensive measures in place to ensure business continuity. Even in the face of unforeseen disruptions, our service to you remains reliable. We maintain up-to-date plans to handle a range of scenarios—from hardware failures to natural disasters. These plans are tested at least annually and audited as part of our ISO 27001 certification.

Our Business Continuity/Disaster Recovery (BC/DR) strategy include the following key elements, as well as best practices designed to keep operations running.

High Availability Architecture

Critical components of the solution are deployed in a highly available manner with multiple instances, clusters, and failover capabilities to withstand individual failures. The infrastructure— computing, storage, databases—across the primary data center has built-in redundancy so that a single hardware or software failure will not take down the service.

Geo-Redundant Disaster Recovery

As noted in the Service Resilience and Data Redundancy section, we maintain a secondary, geographically distant region that can take over in case the primary region becomes unusable. Data is continuously replicated to this DR site. In an emergency, we can activate the secondary environment to restore service, meeting the defined RPO/RTO targets. This protects against region-wide issues, such as natural disasters or major outages.

Frequent Backups

ToolsGroup performs daily backups of both infrastructure state and customer application data. We retain multiple copies of backups for 15 days (rolling), and these backups are stored in an encrypted, geo-distributed storage. The backups ensure that even in a worst-case scenario, like a failure of primary region, your data can be recovered from a recent restore point.

Continuous Monitoring and Alerting

Our operations center monitors system health metrics and security events around the clock. Automated alerts flag any anomalies or signs of trouble, whether it's a hardware issue, a spike in latency, or a security incident. This allows us to respond immediately to incidents that could impact continuity. For example, if an unusual event suggests a potential outage risk, engineers are engaged to mitigate it before it escalates. This proactive stance is critical to preventing small issues from becoming downtime events.

Layers of Contingency

Taken together, these capabilities ensure that ToolsGroup's service remains resilient. Even if the unexpected happens, we have layers of contingency: local redundancy handles component failures, multi-region failover handles large-scale disasters, and backups guard against data corruption or loss. Our customers rely on our platform for mission-critical operations, so we have engineered and governed it to be available when you need it.

+ Security Incident Management

In the unfortunate event of a security incident, ToolsGroup is prepared to respond swiftly and effectively. We have established detailed security incident response policies and procedures that guide our actions from the moment an incident is detected through resolution and post-incident analysis.

The primary goals of our incident management process are:

1. **Detect incidents early**
2. **Minimize incident impact**
3. **Protect customer data**
4. **Communicate transparently with affected parties**

Our robust incident management program has several key facets that minimize impact on business operations.

Incident Response Plan

We maintain a formal incident response plan that defines the exact steps to take when an incident occurs. This plan covers incident identification, classification to gauge severity/impact, containment to stop any further damage or spread, eradication of the threat, recovery of systems, post-incident review and communication with affected parties and authorities. It provides checklists and assignments so that nothing is overlooked during the stress of an incident.

Dedicated Roles and Responsibilities

Specific individuals and teams are assigned security roles. For example, we have an Information Security Manager who leads the incident response efforts, heading a cross-functional Incident Response Team that includes engineering, operations, legal and communications personnel. We have clearly defined responsibilities and an escalation path that includes executive oversight to ensure accountability and proper authority during incident handling.

Rapid Detection and Response

Our monitoring systems— SIEM, alerts, and others described previously— are a crucial first line of defense in detecting incidents. Once an alert or report is received, our security team operates under an on-call rotation to investigate immediately. We aim for prompt detection and assessment so that we can contain any incident as quickly as possible. We also have a process to gather forensic data, such as log analysis and system snapshots, to understand the scope of an incident.

Customer and Authority Notification

ToolsGroup is committed to transparency.
If a data breach or any security incident affecting customer data were to occur, we pledge to notify the impacted customers without undue delay, after first taking steps to secure the environment.
We also coordinate with legal authorities and regulators as required. Our plan's communication component ensures that both customers and relevant authorities are kept informed in a timely and appropriate manner.

Continuous Improvement

After any incident is resolved, we perform a thorough post-mortem analysis to identify lessons learned. We update our security measures and incident response procedures based on the post-mortem results, following a philosophy of continuous improvement. Even in the preferrable absence of incidents, we periodically review and test our incident response plan through drills and tabletop exercises to refine it to incorporate up-to-date best practices and counter emerging threats.

By having a robust incident management program, ToolsGroup ensures that if something goes wrong, the situation will be handled in a professional, effective manner that minimizes risk and impact for our customers. We take pride in fostering trust and having deep care for our customers, which means being ready to respond to the unexpected and being honest and forthright about what we're doing to keep you secure.

+ Compliance and Certifications

Compliance is a cornerstone of ToolsGroup's security program, helping provide assurance to our customers that we meet high standards and follow through on our security commitments. ToolsGroup adheres to both international and local regulations relevant to our services, and we maintain certifications for key security standards widely recognized in the industry.

ISO 27001

ToolsGroup is certified under the ISO/IEC 27001:2022 standard for our Information Security Management System (ISMS). ISO 27001 is a rigorous international standard that specifies how an organization should manage and protect information. We undergo annual third-party audits to maintain this certification, ensuring continuous compliance and improvement. For customers and prospects, we are happy to provide our ISO 27001 certificate and the Statement of Applicability, which details the set of controls in our ISMS, upon request.

Other Security Standards and Frameworks

In addition to ISO 27001, ToolsGroup aligns with other relevant standards and frameworks:

- **SOC 2:** While ToolsGroup itself is not SOC 2 certified, we have incorporated many SOC 2 aligned controls regarding security, availability, confidentiality principles in our operations, and we can support customer due diligence requests around these controls. It's important to note that our underlying cloud providers are SOC 2 certified and can provide evidence of SOC certification upon request.

- **GDPR and Privacy:** For customers operating in the EU or handling personal data, ToolsGroup ensures that our services support GDPR compliance. We act as a Data Processor under GDPR and have measures for data protection and breach notification. ToolsGroup offers Data Processing Agreements with Standard Contractual Clauses for international data transfers as needed. Our privacy program is designed to uphold individuals' data rights and secure personal data according to GDPR and other local privacy laws.

- **Other Regulatory Requirements:** We meet obligations for industry-specific needs, such as supporting 21 CFR Part 11 compliance for customers in life sciences requiring audit trails, and we stay prepared to proactively comply with evolving cloud security certifications. Our cloud hosting partners maintain certifications like FedRAMP High for U.S. government use, SOC 1/2/3, ISO 27017/27018 on cloud security and privacy extensions, and more. By extension, our platform benefits from those compliance protocols at the infrastructure level.

Culture of Compliance and Security

ToolsGroup fosters a culture of compliance and ethics internally. We have an internal Information Security Management System based around the policies, procedures, and guidelines that underpin our ISO 27001 program that is regularly updated and distributed to all employees. This includes security policies, acceptable use rules, secure development practices, and so forth. All staff are required to undergo security training and to follow these policies in their daily work.

Our management demonstrates strong support for security and compliance initiatives, ensuring that we allocate resources and attention to uphold these standards. **Compliance is not a checkbox for us; it's an ongoing commitment** to doing things the right way, bolstering trust between ToolsGroup and our customers.

+ About ToolsGroup

ToolsGroup helps leaders **deliver on their promises when others can't**.

In a world of constant volatility, traditional planning breaks. We **don't try to predict** our way out of uncertainty. We **guide you through it**. ToolsGroup is an ambient supply chain operating system that **quietly steers performance**. Leaders set the targets– cost, service, margin– and the system continuously guides the decisions to get there.

The result is **unparalleled control over demand and supply– and the confidence to deliver certainty, even when conditions change**.

To learn more, visit **www.toolsgroup.com** or follow us on our social channels for the latest updates.

We are committed to delivering innovation with security, so our customers can focus on their business with peace of mind.

toolsgroup®

toolsgroup.com