Metroscope Trust Center

Built for trust. Secured by design.

At Metroscope, trust is not a box to check — it's a principle embedded in every layer of our company and of our product. As a cybersecurity-first SaaS provider working with highly sensitive industrial data, we know that security and transparency are inseparable from our clients' success.

Our product and operations are designed to exceed the expectations of the most demanding industries. Below, we explain how our architecture, culture, and processes ensure that your data is safe, resilient, and handled responsibly.

A cloud-native solution designed for cybersecurity

From day one, Metroscope has been cloud-native, building on the security foundations of Microsoft Azure. Our approach goes beyond basic hosting: cybersecurity is woven into our architecture, operations, and client delivery.

- Architecture: Our platform is deployed in Azure Kubernetes Service (AKS) clusters, ensuring scalability, compute isolation, and strong tenant separation.
- Data protection by design: Every client benefits from segregated databases, dedicated identity and access management, and project-level restrictions.
- Regional flexibility: Clients choose their hosting region (France, Western Europe, or the US).
- Defense-in-depth: We leverage Microsoft Defender, Azure Secure Score, and native monitoring services to continuously harden our environment.

Secure by default

- Encryption everywhere: TLS 1.2+ for data in transit, AES-256 for data at rest.
- Access controls: RBAC, least privilege principles, segregation of duties, and quarterly access reviews.
- Authentication safeguards: SSO and IP whitelisting.
- Continuous reviews: Regular audits of accounts, permissions, and configurations.

Secure by culture

- Dedicated leadership: A Security Lead oversees our ISMS.
- Employee training: All employees receive training on cybersecurity risks.
- Secure development lifecycle: Security checks in each stage of product development.
- Independent validation: Annual penetration tests and third-party reviews.

Minimizing third-party risk

- Data minimization: We only collect the data strictly necessary.
- Controlled reuse: A select group of engineers may reuse data under strict governance.
- No email transfers: Confidential data is exclusively shared through secure channels.
- Environment separation: Infrastructure, applications, and tools fully segregated per client.

Security across the data lifecycle

- Collection: Minimal, purpose-driven, and consent-based.
- Storage: Encrypted on Azure Blob and SharePoint, with regional controls.
- Access: Strictly role-based, least privilege, IP-filtered, and reviewed quarterly.
- Reuse: Permitted only for internal improvement of models.
- Deletion: Permanent, achieved by destroying encryption keys.

Our policies and documentation

We maintain a library of audit-ready documentation to support procurement, compliance reviews, and client due diligence. Policies include:

- Information System Security
- Client Data Protection
- Acceptable Use
- GDPR Compliance
- Digital Asset Management
- Cybersecurity Training
- Logging & Monitoring
- Network Defense
- Physical Security
- Business Continuity & Disaster Recovery
- Laptop Lifecycle
- Use of Cloud Services
- Entra ID Management
- Microsoft 365 Collaboration
- Vulnerability & Threat Management
- Secure SDLC
- Secure API Exposure
- Incident Management

Collaboration and custom hosting

Metroscope's standard hosting already meets the security requirements of the most demanding sectors. But every organization is unique — if your security framework requires specific measures, our teams are ready to adapt.

Contact our team for documentation or a tailored solution.