LAMERS TOOLING BV

Data Protection & Cybersecurity Guidelines

Bij Lamers Tooling b.v. is vertrouwelijkheid, integriteit en beschikbaarheid van data de basis van onze dienstverlening. Vanwege de aard van onze projecten en de sectoren waarin wij actief zijn (Semicon, Defensie, Aerospace), hanteren wij strikte richtlijnen voor databescherming en informatiebeveiliging.

- **Wettelijke naleving:** Wij verwerken alle persoonsgegevens en bedrijfsgevoelige data in strikte overeenstemming met de Algemene Verordening Gegevensbescherming (AVG/GDPR) en toepasselijke nationale veiligheidskaders.
- **Informatiebeveiliging (Security by Design):** Onze interne systemen en processen zijn ingericht volgens internationaal erkende standaarden voor informatiebeveiliging (zoals ISO 27001 / NIST). Dit omvat onder andere strikt toegangsbeheer (Need-to-Know principe), end-to-end encryptie en continue monitoring van onze IT-infrastructuur.
- **Geheimhouding & Toeleveringsketen:** Al onze medewerkers en toeleveranciers zijn gebonden aan strikte, project specifieke geheimhoudingsovereenkomsten (NDA's). Data van klanten wordt strikt gescheiden opgeslagen en nooit zonder expliciete, contractuele toestemming gedeeld met derden.
- **Fysieke en Organisatorische Veiligheid:** Naast digitale barrières handhaven wij strikte fysieke toegangsbeveiliging op onze locaties en trainen wij ons personeel doorlopend op het gebied van security awareness en cybersecurity-risico's.

Om operationele en veiligheidsredenen publiceren wij geen specifieke technische details, netwerkarchitecturen of beveiligingsprotocollen op onze openbare website. Voor geautoriseerde relaties en auditdoeleinden zijn gedetailleerde compliance documenten op aanvraag en onder NDA beschikbaar.

Jos Lamers, CEO 14-09-2026

Data Protection & Cybersecurity Guidelines

At Lamers Tooling b.v., confidentiality, integrity and the availability of data form the basis of our services. Due to the character of our projects and the sectors in which we operate (semiconductors, defence, aerospace), we adhere to strict guidelines on data protection and information security.

- **Regulatory Compliance:** We process all personal and proprietary business data in strict accordance with the General Data Protection Regulation (GDPR) and applicable national security frameworks.
- **Information Security (Security by Design):**
  Our internal systems, infrastructure, and workflows are aligned with internationally recognized information security standards (such as ISO 27001 / NIST). This includes strict identity and access management (based on the Need-to-Know principle), end-to-end data encryption, and continuous monitoring of our IT environment.
- **Confidentiality & Supply Chain Integrity:** All employees, contractors, and partners are bound by comprehensive, project-specific Non-Disclosure Agreements (NDAs). Customer data is strictly segregated and is never shared with third parties without explicit, contractual authorization.
- **Physical & Organizational Security:** Beyond digital safeguards, we enforce strict physical access controls at our facilities. Furthermore, our workforce undergoes ongoing security awareness training to mitigate cybersecurity risks and insider threats.

For operational security (OPSEC) and confidentiality reasons, we do not publish specific technical details, network architectures, or internal security protocols on our public website. Detailed compliance documentation can be made available to authorized parties for audit purposes upon request and subject to an NDA.