ILF GROUP INFORMATION SECURITY POLICY

ILF stands for trusted delivery of services via a secure working environment

1. Our Commitment

- Information Security is a top priority at ILF. Availability, integrity and confidentiality of information are essential assets and form the fundamental basis for our services. We are committed to protecting information, data and information systems in an effective manner.
- Our commitment is reflected in related processes, standards and procedures, including aspects concerning data protection, acceptable use, access control, incident reporting, business continuity, supplier management and compliance.
- Information Security processes are implemented through a risk-based approach, clear governance, defined responsibilities and continuous improvement. Applied measures consider an appropriate balance of business requirements, innovation opportunities and evolving cyber security risks.

2. Information Security Standards

- We live Information Security as a shared responsibility. All staff members are expected to handle information carefully, comply with applicable processes and procedures and contribute to a security-aware culture through responsible behaviour and regular subject-matter training.
- We identify, assess and treat Information Security risks in a structured and proactive manner, and apply appropriate technical, organizational and physical controls.
- Information and data processed at ILF is protected in accordance with applicable laws, governmental regulations, contractual obligations and ILF-internal requirements.
- Secure technology, system architecture and IT operations are key to reliable and resilient services. ILF applies appropriate security measures for identities, devices, networks, services, applications and data.
- External service providers, contractors and partners accessing ILF information are required to adhere to our applicable standards. Information Security requirements are considered during selection, contracting, onboarding, monitoring and termination of third-party relationships.
- Effective incident management and business continuity capabilities are maintained to detect, report, assess, contain and recover from information security incidents or disruptions in a timely manner.
- The effectiveness of applied measures and controls is monitored through reviews, audits and focused performance indicators. A structured lessons-learned approach is applied for constant improvement.

3. Scope

- This policy applies to all directors, managers and employees of all ILF Group companies.

Digitally signed by Laesser, Klaus
Date: 13/August/2026

Klaus Lässer,
Chief Executive Officer

Digitally signed by Wasilewski, Marcin
Date: 2026.08.05

Marcin Wasilewski,
ILF Group Information Security Officer